ANTI-MONEY LAUNDERING

COMPLIANCE POLICY

FOR

PELICAN EXCHANGE EUROPE (CY) LTD

Revision History

Policy Name	**Anti-Money Laundering Compliance Policy**
Version Number	**1.0**
Date Approved	
Effective Date	**02/05/2023**
Policy Owner	**Pelican Exchange Europe (CY) Ltd**
Policy Approver	**Pelican Board of Directors**

Table of Contents

Policy Statement

It is the policy of Pelican Exchange Europe (CY) Ltd to implement and comply with applicable legal requirements, including those related to anti-money laundering. To this end, Pelican Exchange Europe (CY) Ltd is committed to establishing and maintaining policies, procedures, and internal controls reasonably designed to achieve compliance with its implementing regulations.

To achieve this goal, the company has established this policy.

1. GENERAL DEFINITIONS

For the purposes of this Manual, unless the context shall prescribe otherwise:

"**Advisory Authority**" means the Advisory Authority for Combating Money Laundering and Terrorist Financing which is established under Section 56 of the Prevention and Suppression of Money Laundering Activities Law of 2007 to 2022, as amended from time to time.

"Advisory Committee on Economic Sanctions" means the Financial Sanctions Consultative Committee which was established by decision of the Council of Ministers May 25, 2012, chaired by the Minister of Finance, deals with requests for release of funds that have been committed on the basis of Sanctions and Restrictive Measures, and makes suggestions accordingly for approval or rejection by the final decision to be taken by him Minister of Finance.

"**Beneficial Owner**" means the natural person or natural persons, who ultimately owns or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted. The Beneficial Owner shall at least include:

(a) In the case of corporate entities:

(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the Client held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the Client held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control.

Control through other means may be determined, inter alia, in accordance with the criteria of Sections 142(1)(b) and 148 of the Companies Law, as applicable.

(ii) If, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged

entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point.

(b) In the case of trusts:

i. The settlor,
ii. The trustee,
iii. The protector, if applicable,
iv. The beneficiary or, where the person who is the beneficiary of the legal arrangement or of the legal entity has not yet been identified, the category of persons in the interest of which the legal arrangement or legal entity is or has been established,
v. Any other natural person who exercises the ultimate control of the trust through direct or indirect ownership or by other means.

In the case of legal entities, such as foundations and legal arrangements similar to trusts, includes the natural person holding a corresponding or similar position with a person referred to in paragraph (b) above.

"Board of Directors" means the board, committee, and / or body of an entity, which has the power to determine the strategy, objectives, and general direction of that entity and to oversee the management decision-making process, including the person who actually runs the business of that entity.

*"***Business Relationship***"* means a business, professional or commercial relationship between the Client and the Company and which is connected with the professional activities of the Company and which is expected, at the time when the contact is established, to have an element of duration.

"**Client**" means any legal or physical person aiming to conclude a Business Relationship or being offered a one-off service with the Company. Counterparties are also treated as Clients only when the Company is executing a Client order by entering into a private Over-the-Counter deal/transaction (e.g. buying and selling) directly with the Counterparty.

"**Company**" means Pelican Exchange Europe (CY) Ltd which is incorporated in the Republic of Cyprus with registration number **HE 426432.**

"Correspondent Relationship" means:

(a) the provision of banking services by one bank ('correspondent') to another bank ('respondent'), including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;
the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

"Credit Institution" has the meaning given to the term in Article 4, Paragraph 1, Subparagraph 1 of the Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, and includes a credit institution to which a licence to operate as an authorised credit institution (ACI) pursuant to the provisions of the Business of Credit Institutions Law and a credit institution which operates in the Republic of Cyprus pursuant to provisions of Section 10A of the Business of Credit Institutions Law.

"Criminal Activity" means the offenses referred to in Section 5 of the Law.

"CySEC" means the Cyprus Securities and Exchange Commission established and operating pursuant to the Cyprus Securities and Exchange Commission (Establishment and Responsibilities) Law.

"**Directive**" means theDirective of 2020 of CySEC for the Prevention and Suppression of Money Laundering and Terrorist Financing, as this has been amended from time to time

"**European Economic Area (EEA)**" means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.

"**EU Directive**" means Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.

"Electronic money" means monetary value stored in electronic form, including magnetically form, as represented by a claim on the electronic money issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer. Please refer to Article 2 of the Electronic Money Law. Electronic Money is money stored in a bank's debit or credit card and electronic e-wallets such as paypal. Electronic money has the following characteristics: 1. Electronic money and cash can be easily converted directly to each other; 2. The number of electronic money corresponds to the same amount of physical currency; 3. We need to pay the physical currency to the issuer of electronic money (banks and other financial institutions) in exchange for the same amount of electronic money.

"Financial Institution" means:

a. an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14) and (15) of Annex IV of the Business of Credit Institutions Law, including the activities of currency exchange offices (bureaux de change)
b. an insurance or reinsurance undertaking within the meaning given to the term by Section 2 of the Insurance and Reinsurance Business and Other Related Issues Law, insofar as it carries out life assurance activities covered by the scope of the said Law

c. an investment firm or IF within the meaning given to the term by Section 2(1) of the Investment Services and Activities and Regulated Markets Law (L.87/2017), as this has been amended from time to time
d. a collective investment undertaking marketing its units or shares
e. an insurance or reinsurance intermediary within the meaning given to the term by Section 356 of the Insurance and Reinsurance and Other Related Issues Law where it acts with respect to life insurance and other investment-related services
f. branches, of any of the financial institutions as referred to in points (a) to (e), when they are in Cyprus, whether their head office is situated in a Member State or in a third country.

"Financial activities" includes the following:

a. Exercise of professional activities by auditors, external accountants and tax advisors, including transactions for the account of their Clients in the context of carrying out financial business.
b. Exercise of professional activities as independent lawyer, with the exception of privileged information, when they participate, whether:
   (i) by assisting in the planning or execution of transactions for their Clients concerning the:
      - buying and selling of real property or business entities,
      - managing of Client money, securities or other assets,
      - opening or management of bank, saving or securities accounts,
      - organisation of contributions necessary for the creation, operation, or management of companies,
      - creation, operation or management of trusts.
   (ii) By acting on behalf and for the account of their Clients in any financial or real estate transaction.
c. Dealing in real estate transactions, conducted by Real Estate Agents, according to the provisions of the Real Estate Agents, according to the provisions of the Real Estate Agents Law, which are from time to time in force.
d. The following trust services and company services to third parties:
   (i) forming companies or other legal persons,
   (ii) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons,
   (iii) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement,
   (iv) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement,
   (v) acting as or arranging for another person to act as a nominee shareholder for another person, and

(vi) any of the services or activities specified in Section 4 of the Regulating Companies Providing Administrative Services and Related Matters Law, as amended or replaced.

e. Gaming/gambling service providers as provided by the applicable legislation of the Republic of Cyprus.

"Gambling Services" means a service which involves wagering a stake with monetary value in games of chance, including those with an element of skill such as lotteries, casino games, poker games and betting transactions that are provided at a physical location, or by any means at a distance, by electronic means or any other technology for facilitating communication, and at the individual request of a recipient of services.

"**goAML Professional Edition (PE)**"means an IT system implemented by the Money Laundering Combat Unit of the Republic (hereinafter the "**Unit**") and used by the Company for the online submission of Suspicious Activities Reports and Suspicious Transactions Reports.

"**Group"** means a group of undertakings which consists of a parent undertaking, its subsidiaries, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU

"Guidelines" or **"the Risk Factors Guidelines"** or **"the Risk-Based Supervision Guidelines"** means the EBA Guidelines on the characteristics of a risk-based approach to anti- money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/849 (amending the Joint Guidelines ESAs 2016/72).

High Risk Third Country" 'high risk third country' means:

(i) a third country, designated by the European Commission pursuant to the provisions of article 9 (2) of the 4th EU Directive by the issuance of acts by way of derogation, which presents strategical shortcomings in its national system for combating ML and TF which are considered as important threats for the financial system of the European Union, and

(ii) a third country, which is categorised by the obliged entities as high risk in accordance with the risk assessment foreseen by article 58A of the AML/CFT Law.

"**Investment and Ancillary Services**" means the investment and ancillary services as per the First Appendix of the Investment Services and Activities and Regulated Markets Law (L.87/2017), as this has been amended from time to time, for which the Company is licensed by CySEC to offer.

"**Law**" means the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 – 2022 as amended from time to time.

"**Manual**" means the Company's Risk Management & Procedures Manual (this manual), according to the Directive.

"Member of the Unit for the Implementation of Sanctions", in the Financial Sector in relation to Sanctions imposed by UN Security Council Resolutions and Restrictive Measures imposed by European Union (EU) Council Regulations, as per Council of Ministers Decision dated 25 February 2016.

"MOKAS" or **"Unit"** means the Unit for Combating Money Laundering and established under Section 54 of the Law. MOKAS is the Financial Intelligence Unit (**"FIU"**) of Cyprus, and it is the national centre for receiving, requesting, analysing and disseminating disclosures of suspicious transactions reports and other relevant information concerning suspected money laundering and terrorist financing.

"**Money Laundering**" means the money laundering offences defined in Section 4 of the Law, referred to also the following.

1. Every person who (a) knows or (b) at the material time ought to have known that any kind of property constitutes proceeds from the commission of a *predicate offence* as this is defined in Section 5 of the Law, carries out the following activities:
    i. converts or transfers or removes such property, for the purpose of concealing or disguising its illicit origin or of assisting in any way any person who is involved in the commission of the predicate offence to carry out any of the above actions or acts in any other way in order to evade the legal consequences of his actions,
    ii. conceals or disguises the true nature, the source, location, disposition, movement of and rights in relation to, property or ownership of this property,
    iii. acquires, possesses or uses such property,
    iv. participates in, associates, co-operates, conspires to commit, or attempts to commit and aids and abets and provides counselling or advice for the commission of any of the offences referred to above,
    v. provides information in relation to investigations that are carried out for laundering offences for the purpose of enabling the person who acquired a benefit from the commission of a predicate offence to retain the proceeds or the control of the proceeds from the commission of the said offence,
    vi. commits an offence punishable by fourteen years' imprisonment or by a pecuniary penalty of up to EUR 500.000 or by both of these penalties in the case of (a) above and by five years' imprisonment or by a pecuniary penalty of up to EUR 50.000 or by both in the case of (b) above.

2. Further and for the purposes of point 1 above:
    (a) It does not matter whether or not the predicate offence is subject to the jurisdiction of the Cyprus Courts,
    (b) Laundering offenses may also be committed by perpetrators of predicate offences,
    (c) The knowledge, intent or purpose required as elements of the offenses referred above, may be inferred/concluded from objective factual circumstances

(d) No previous or simultaneous conviction for predicate offense from which the proceeds resulted is required.
(e) It is not required to verify the identity of the person who has committed the predicate offence from whom the proceeds have originated.

"Predicate Offences" is any offence which is defined as a criminal offence by a law of the Republic.

"Occasional Transaction" means any transaction other than a transaction carried out in the course of an established Business Relationship formed by a person acting in the course of financial or other business.

"Obliged Entities" means the following persons that the provisions of the Law apply to and which include:

(a) credit institutions;
(b) financial institutions;
(c) the following natural or legal persons acting in the exercise of their professional activities:
    i. auditors, external accountants and tax advisors and any other person who undertakes, either directly or through other persons with whom that person attached, material assiastance, assistance or advice on tax matters, as the main business or professional, activity;
    ii. independent legal professional, when it participates, whether acting on behalf of a Client in a financial or real estate transaction, or by assisting in the planning or carrying out of a transaction for its Client concerning the:
        - buying and selling of real property or business entities;
        - managing of Client money, securities or other assets;
        - opening or management of bank, savings or securities accounts;
        - organisation of contributions necessary for the creation, operation or management of companies;
        - creation, operation or management of trusts, companies, foundations, or similar structures;
(d) Natural or legal person not already covered under point (c) above, offering the following services to trusts or companies:
    i. the formation of companies or other legal persons
    ii. acting as, or arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
    iii. providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement
    iv. acting as, or arranging for another person to act as, a trustee or a trustee of express trusts or a similar legal arrangement
    v. holding the shareholding capital of corporate entities and registering such shareholder in the respective registers of registered shareholders on behalf of or

on account of third parties, other than a company listed on a regulated market that is subject to disclosure requirements in accordance with European Union law or subject to equivalent international standards, or ensures that other person exercises respective duties; and

(e) any of the services or activities specified in Section 4 of the Regulation of Administrative Service Providers and Related Issues Law.

(f) estate agents

(g) providers of gambling services, as provided in the relevant laws of the Republic

(h) person who trades, provided that the payment is made or received in cash and amounts to ten thousand EURO (€10,000) or more, whether the transaction is carried out in a single transaction or in several operations which appear to be linked.

(i) providers of Services related to Crypto Assets, which are registered in the register provided for in paragraph (1) of Section 61E of the Law.

(j) persons, whose supervision is assigned to the Cyprus Securities and Exchange Commission in accordance with the provisions of the Cyprus Securities and Exchange Commission Law or any other Law.

(k) persons who trade or act as intermediaries in the trade of works of art, including of cases where this takes place by art galleries and auction houses, provided that the value of the transaction or series of related transactions amounts to or exceeds ten thousand EUR (€10,000).

(l) persons who store, trade or act as intermediaries in the trade of works of art carried out from free ports, if the value of the transaction or series of related transactions amounts to or exceeds ten thousand euros (€10,000).

"Other Business Activities" includes the following trust services and company services to third parties:

a. forming companies or other legal person
b. acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons
c. providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement
d. acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement
e. acting as or arranging for another person to act as a nominee shareholder for another person, and
f. any of the services or activities specified in Section 4 of the Law regulating Companies providing Administrative Services and Related Matters of 2012, as this has been amended from time to time.

"Property" means assets of any kind, whether corporeal or incorporeal, movable assets including cash, immovable assets, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such asset.

"**Politically Exposed Person (PEP)**" means the natural person to whom or who has been entrusted with prominent public function in the Republic or in another country and his/her immediate family members and persons known to be close associates of such person (see also points 4 - 7 of Section 10.8.6 of the Manual).

"**Republic**" means the Republic of Cyprus.

"**Regulated Market**" means the multilateral system managed or operated by a market operator and which brings together or facilitates the bringing together of multiple third-party buying or/and selling interests in financial instruments - in the system and in accordance with its non-discretionary rules - in a way that results in a contract, in respect of the financial instruments admitted to trading under its rules or/and systems, and which is authorised and functions regularly in accordance with the provisions of the Law 87(I)/2017 or respective legislation.

"Senior Management" means an officer or an employee of the Company with sufficient knowledge of the Company's risk exposure to the Money Laundering and Terrorist Financing and with sufficient seniority to take decisions affecting its risk exposure. The Senior Management is not, in all cases, required to be a member of the Board of Directors of the Company. The *Senior Management* of the Company is responsible for approving the policies, procedures and controls applied by the Company as well as monitor them and, where necessary, enhancing the measures taken.

"**Shell Bank**" means a credit institution or financial institution, or an institution engaged in equivalent activities incorporated in a jurisdiction which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

"Terrorist Financing" means the provision or gathering of funds by any means, directly or indirectly, with the intention to use such funds or knowing that they will be used in whole or in part for the commission of an offence within the meaning given to the term by section 4 of the International Convention for the Suppression of the Financing of Terrorism (Ratification and Other Provisions) Law and by sections 5 to 13 of the Combating of Terrorism Law.

"**Third Country**" means the country which is not a member of the European Union or contracting party to the European Economic Area Agreement, signed in Oporto on the 2nd of May 1992 and adjusted by the Protocol signed in Brussels on the 17th of May 1993, where the Agreement is thereafter, amended.

2. INTRODUCTION

The purpose of the Manual is to lay down the Company's internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing.

The Manual is developed and periodically updated by the Money Laundering Compliance Officer (hereinafter the "**MLCO**") based on the general principles set up by the Company's Board of Directors (hereinafter the "**Board**") in relation to the prevention of Money Laundering and Terrorist Financing.

All amendments and/or changes of the Manual must be approved by the Board and the Senior Management.

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 on boarding of Clients and for the application of the practices, measures, procedures and controls that have been determined herein.

The Manual has been prepared to comply with the provisions of the Law, the Directive of CySEC and the Combating of Terrorism and Victim Protection Law of 2019 (75(I)/2019).

3. THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

3.1. General

The responsibilities of the Board in relation to the prevention of Money Laundering and Terrorist Financing include the following:

(a) to determine, record and approve the general policy principles of the Company in relation to the prevention of Money Laundering and Terrorist Financing and communicate them to the MLCO
(b) 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 the MLCO and, where is necessary, assistant MLCOs and determine their duties and responsibilities, which are recorded in this Manual
(c) to approve the Manual
(d) to ensure that all relevant requirements of the Law and of the Directive are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement
(e) to ensure that the MLCO, the Alternate MLCO and his assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of Money Laundering and Terrorist Financing (i.e. personnel of the Administration/Back Office Department), have complete and timely access to all data and information concerning Clients' identity, transactions' 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
(f) to ensure that all employees are aware of the person who has been assigned the duties of the MLCO, as well as his assistants (if any), to whom they report, according to point (e) of Section 6.2 of the Manual any information concerning transactions and

activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing

(g) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the MLCO, either directly or through his assistants, if any, and notifies accordingly the MLCO for its explicit prescription in the Manual

(h) to ensure that the MLCO, the Alternate MLCO, the assistant MLCOs, if any, and the Head of Administration/Back Office Department have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties

(i) to assess and approve the MLCO's Annual Report of Section 7 of the Manual and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report

(j) to meet and decide the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the Internal Auditor's report in the manner described in Section 5 of the Manual. The minutes of the said decision of the Board and the Internal Auditor's report shall be submitted to CySEC within twenty (20) days from the said meeting and no later than four (4) months after the end of the calendar year (i.e. the latest, by the end of April).

(k) to implement adequate and appropriate systems and processes to detect, prevent and deter money laundering arising from serious tax offences.

(l) to ensure that the Company's officials do not knowingly aid or abet Clients in committing tax offences.

(m) Approve the mandatory annual training programme prepared by the MLCO.

(n) to enhance further the AML/CFT measures adopted, when this is deemed necessary

(o) ensure to be adequately trained to be well aware and up-to-date with the regulatory framework and the relevant responsibilities deriving from this.

(p) At least once a year, assess the effective functioning of the AML/CFT compliance function, including by considering the conclusions of any AML/CFT-related internal and/or external audits that may have been carried out, including with regard to the appropriateness of the human and technical resources allocated to the AML Compliance Officer.

(q) The management body in its supervisory function should have access to and consider data and information of sufficient detail and quality to enable it to discharge its AML/CFT functions effectively. At a minimum, the management body in its supervisory function should have timely and direct access to the activity report of the AML Compliance Officer, the report of the internal audit function, the findings, and observations of external auditors, where applicable, as well as the findings of the competent authority, relevant communications with the FIU and supervisory measures or sanctions imposed.

(r) The management body in its supervisory function should be responsible for setting, approving and overseeing the implementation of an adequate and effective internal governance and internal control framework to ensure compliance with applicable requirements in the context of the prevention of money laundering and terrorism financing.

(s) being informed of the results of the business-wide ML/TF risk assessment.
(t) overseeing the implementation of the AML/CFT policies and procedures and the extent to which these are adequate and effective in light of the ML/TF risks to which the financial sector operator is exposed and taking appropriate steps to ensure remedial measures are taken where necessary.
(u) reviewing at least once a year the activity report of the AML/CFT compliance officer and obtaining interim updates more frequently for activities that expose financial sector operators to higher ML/TF risks.
(v) assessing the effective functioning of the AML/CFT compliance function, at least once a year, by assessing, in particular, the adequacy of the human and technical resources allocated to the AML/CFT compliance officer.
(w) implementing the organisational and operational structure necessary to discharge the AML/CFT strategy defined by management body, paying particular attention to the adequacy of the human and technical resources allocated to the AML/CFT compliance officer function, the need for a dedicated AML/CFT unit to assist the AML/CFT compliance officer.
(x) approving the AML/CFT compliance officer's activity report and ensuring its completeness, seriousness and accuracy.
(y) ensuring adequate, timely and sufficiently detailed AML/CFT reporting to the competent authority.
(z) in case certain operational functions of the AML/CFT compliance officer are outsourced, the Management Body shall approve the service provider and ensure that they receive regular reporting from the service provider.

The Company should identify a member of the Board of Directors who will be responsible for the implementation of the Law and of the applicable Directives and/or Circulars and/or Regulations including any relevant acts of the European Union.

4. AML Responsible Director

A member of the Board shall be responsible for the implementation of the provisions of the Law and of the directives and/or circulars and/or regulations issued pursuant thereto including any relevant acts of the European Union.

The Company has appointed an AML Responsible Director and keeps the organization's structure chart up to date in respect to this. More specifically, the AML Responsible Director shall bear the responsibility of, *inter alia*, the following duties **on ongoing basis**:

a. supervising that all requirements of the Law and the relevant CySEC directives and circulars are applied
b. supervising the activities of the personnel of the MLCO function
c. supervising the ongoing implementation of the provisions of the Manual and relevant reporting to MLCO, Risk Manager and/or Board
d. ensuring that there is frequent collaboration between the Board of Directors and the MLCO function

e. supervising that the Manual is updated on an ongoing basis so as to comply with the CySEC's future requirements, as applicable, regarding the Client identification and due diligence procedures
f. understanding and developing knowledge of regulatory guidelines and how they influence Company's business processes with the assistance of the MLCO
g. supervising the duties of the MLCO and, assistant MLCOs and responsibilities, which are recorded in the risk management and procedures manual regarding money laundering and terrorist financing
h. supervising the preparation of the Annual report of the MLCO
i. ensuring that the appropriate means and training is provided to Company's employees in relation to Anti – Money Laundering in order for them to carry out their duties successfully and in compliance with relevant laws and regulations
j. supervising the reports of suspicious transactions to the Unit
k. supervising the preparation of the Monthly Prevention Statement and its submission to CySEC via CySEC's Portal
l. ensuring that the MLCO and his/her assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, shall have complete and timely access to all data and information concerning Clients' identity, transaction documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties
m. supervising the implementation of the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the Internal Auditor's report
n. supervising the implementation of the Client Acceptance Policy (CAP)
o. receiving on periodic basis information from the employees of the Company in relation to the ongoing monitoring of *high risk* Clients' transactions and activities and ensure that the relevant guidance is provided by the MLCO, as and where needed
p. supervising and assessing the correct and effective implementation of the internal practices mentioned in Manual, for the proper and full implementation of the Company's obligations and/or procedures, where the verification of a Client's identity takes place during the establishment of business relationship
q. supervising that the MLCO applies all the appropriate monitoring mechanisms (e.g., on-site visits to different departments of the Company) which will provide him 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
r. supervising that in the event that the MLCO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, he/she gives appropriate guidance for corrective measures and informs the Board accordingly.

Further to the above, the Management Body should ensure that the member of the Management Body who is responsible for the implementation of the laws, regulations and administrative provisions regarding AML:

a. has adequate knowledge, skills and experience regarding the identification, assessment and management of the ML/TF risks, and the implementation of AML/CFT policies, controls and procedures;
b. has a good understanding of the financial sector operator's business model and the sector in which the financial sector operator is operating, and the extent to which this business model exposes the financial sector operator to ML/TF risks;

is informed in a timely manner of decisions that may affect the risks to which the financial sector operator is exposed.

5. OBLIGATIONS OF THE INTERNAL AUDITOR

5.1. General

Depending on the size and nature of the activities of the Company, an independent Internal Audit function should be established for the verification of policies, controls and procedures.

The following obligations of the Internal Auditor are addressed specifically for the prevention of Money Laundering and Terrorist Financing:

(a) the Internal Auditor shall review and evaluate, at least on an annual basis, the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of Money Laundering and Terrorist Financing mentioned in the Manual

(b) the findings and observations of the Internal Auditor, in relation to point (a) above, shall be submitted, in a written report form, to the Board which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected. The Minutes of the above-mentioned decision of the Board and the internal auditor's report are submitted to CySEC within twenty (20) days from the Board of Directors' meeting and no later than four (4) months after the end of the calendar year (i.e., the latest, by the end of April).

6. MONEY LAUNDERING COMPLIANCE OFFICER

6.1. General

The MLCO shall belong hierarchically to the higher ranks of the Company's organisational structure so as to command the necessary authority. The MLCO shall be skilled, knowledgeable and experienced in the financial services or other business activities, as applicable. Furthermore, the MLCO shall lead the Company's Money Laundering Compliance procedures and processes and report to the *Senior Management*. The MLCO shall also have the resources, 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.

In performing his role, the Money Laundering Compliance Officer takes into account the nature, scale and complexity of its business, and the nature and range of investment services and activities undertaken in the course of that business.

The Company, in case of absence of the MLCO, must appoint an Alternate MLCO, who will temporarily replace the MLCO and perform her duties as provided for by the Law and the Directive and satisfy the requirements for the appointment of an MLCO.

The Alternate MLCO will have the same responsibilities as the MLCO during the period she will perform the duties of the MLCO. The Company will proceed to such appointment taking into consideration the level of knowledge and experience of the appointed person together with the ability to perform the duties of the MLCO in the most efficient and effective way.

The MLCO should ensure that she has sufficient authority to propose, on her own initiative, all necessary or appropriate measures to ensure the compliance and effectiveness of the internal AML/CFT measures to the management body in its supervisory and management function.

In addition, the Company will appoint one member (executive or non-executive) of its Board of Directors as the responsible person for the implementation of the legal framework related to the prevention and suppression of money laundering and terrorist financing. The Company's Board of Directors will determine the policies and procedures to ensure the implementation of the provisions of Section 58D of the Law.

6.2. Duties of the MLCO

During the execution of his duties and the control of the compliance of the Company with the Law and the Directive, the MLCO shall obtain and utilise data, information and reports issued by international organisations, as these are stated in Section 8.5 of the Manual.

The duties of the MLCO shall include, *inter alia*, the following:

(a) to design, based on the general policy principles of the Company mentioned in point (a) of Section 6 of the Manual, the internal practice, measures, procedures and controls relevant to the prevention of Money Laundering and Terrorist Financing, 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 Money Laundering and Terrorist Financing (e.g. services and transactions via the internet or the telephone) as well as measures so that the risk of money laundering and terrorist financing 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)

(b) to develop and establish the Client Acceptance Policy according to Section 9 of the Manual and submit it to the Board for consideration and approval

(c) to review and update the Manual as may be required from time to time, and for such updates to be communicated to the Board for their approval

(d) to monitor and assess the correct and effective implementation of the policy mentioned in point (a) of Section 3 of the Manual, the practices, measures, procedures and controls of point (a) above and in general the implementation of the

Manual. In this respect, the MLCO shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him 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 MLCO 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 Board

(e) 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 (hereinafter the "Internal Suspicion Report"), a specimen of such report is attached in Appendix 1 of the Manual

(f) to evaluate and examine the information received as per point (e) above, 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 (e) above shall be done on a report (hereinafter the "Internal Evaluation Report"), a specimen of such report is attached in Appendix 2 of the Manual

(g) if following the evaluation described in point (f) above, the MLCO decides to notify the Unit, then he should:

- complete an online report on the web-application of the Unit, and submit it through the submit Suspicious Activities Reports and Suspicious "**goAML Professional Edition (PE)**" (https://reports.mokas.law.gov.cy/live/Home), the soonest possible, given that the Company has already registered with the relevant reporting system of the UNIT, or
- Complete an XML Report which is compatible with the XML schema as per the requirements of the Unit, and submit it through the "**goAML Professional Edition (PE)**" (https://reports.mokas.law.gov.cy/live/Home), given that the Company has already registered with the relevant reporting system of the UNIT. It is provided that, after the submission of the MLCO Report to the Unit, the accounts involved and any other connected accounts, are closely monitored by the MLCO and following any directions from the Unit, thoroughly investigates and examines all the transactions of the accounts, as applicable and relevant to the Investment and Ancillary Services being offered by the Company
- The Unit will no longer provide interim or closing feedback on each STR/SAR submitted. The feedback policy of the Unit is as follows:
    - Each electronically submitted STR/SAR will receive automatic acknowledgment of receipt, along with a corresponding reference number.
    - As soon as an investigator is assigned to the STR/SAR by the Unit, the Company shall be informed accordingly.
    - In exceptional cases and when deemed necessary by the Unit or if requested by the Company, feedback on specific cases, interim and /or final, will be provided.

- If administrative orders for postponement of transactions or for the monitoring of bank accounts is considered necessary, the Company will be informed accordingly.
- Periodically, the Unit will issue and distribute to the Company a report which will consist of sanitized cases, trends, indicators, and statistics.
- The Annual Report of the Unit will be published and distrusted to the Company.
- Further to the above, the MLCO shall be responsible to monitor this procedure and take appropriate actions.

(h) if following the evaluation described in point (f) above, the MLCO decides not to notify the Unit then he should fully explain the reasons for such a decision on the MLCO's Internal Evaluation Report

(i) to act as a first point of contact with the Unit, upon commencement of and during an investigation as a result of submitting a report to the Unit according to point (g) above

(j) to ensure the preparation and maintenance of the lists 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

(k) 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

(l) to evaluate the systems and procedures applied by a third person on whom the Company may rely for Client identification and due diligence purposes, according to Section 10.10 of the Manual, and approves the cooperation with it

(m) to establish, review and evaluate the procedures in order to satisfy the completeness, validity and reliability of the information the Company has access, in the course of an electronic verification, according to Section 14.2 of this Manual.

(n) to ensure that the branches and subsidiaries of the Company, if any, that operate in countries outside the EEA, have taken all necessary measures for achieving full compliance with the provisions of the Manual, in relation to Client identification, due diligence and record keeping procedures

(o) to provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing

(p) 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 money laundering or terrorist financing as applicable and relevant to the services being offered by the Company

(q) to determine whether the Company's departments and employees that need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organises appropriate training sessions/seminars. In this respect, the MLCO prepares and applies an annual staff training program according to Section 15.2

of the Manual. Also, the MLCO assesses the adequacy of the education and training provided

(r) to prepare correctly and submit timely to CySEC the monthly prevention statement of Section 7.2. of the Manual and provide the necessary explanation to the appropriate employees of the Company for its completion

(s) to prepare the Annual Report, according to Section 7 of the Manual

(t) to respond to all requests and queries from the Unit and CySEC, provide all requested information and fully cooperate with the Unit and CySEC

(u) to maintain a registry which includes the reports of points (e), (f) and (g), and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the MLCO, date of assessment, date of reporting to the Unit), the evaluation reports of point (d) and all the documents that verify the accomplishment of his duties.

(v) to monitor and assess the correct and effective implementation of the internal practices mentioned in Section 10.4.2 of the Manual, for the proper and full implementation of the Company's obligations and/or procedures, where the verification of a Client's identity takes place during the establishment of business relationship. In this respect, the MLCO shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him 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 MLCO shall identify 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 Board.

a. to freeze all funds, financial assets and financial resources belonging to or controlled by a designated person or entity, owned or controlled in whole or in part, directly or indirectly, by a designated person or entity, derive or stem from funds or other assets owned or controlled, directly or indirectly, by a designated person or entity, owned or controlled by a person or entity, acting on behalf of, or following instructions by a designated person or entity.

b. in case the Company discovers that it is in possession or control of or is otherwise dealing with the funds or economic resources of a designated person, then it is required: (i) to freeze the assets immediately (ii) not deal with them or make them available to or for the benefit of the designated person (iii) report to the Commission

c. if following the evaluation described in point (y) above, the MLCO must report to CySEC as the Supervisory Authority, who will, in turn, report to the Ministry of Foreign Affairs, any assets that have been frozen or any action taken in relation to compliance with the restrictive measures of the European Union and the sanctions of the Security Council of the United Nations, as referred to in Section 25 of Law 75(I)/2019. If the Company fails to comply with the provisions of Sections 23 or 24 of the Law 75(I)/2019 then CySEC may take the measures as provided for in Section 59(6) of the Law

d. to identify and assess the sanctions risks to which the Company it is exposed and implement a sanctions screening programme in line with its nature, size and complexity. Sanction screening is a control used to detect, prevent and manage

sanctions risk. Systems should be in place to detect newly designated sanctioned individuals and to prevent dissipation of assets

e. to implement a sanctions screening programme created in line with the AML/CFT Program which should include:
   (i) Policies: the requirements as to when screening needs to be done and at which frequency, how alerts should be handled and especially how to deal with the alerts if not enough information is available.
   (ii) Responsible person: Potential sanctions matches should be reviewed by person with appropriate skills and experience. The staff should be properly trained to know how to deal with potential sanctions matches.
   (iii) Risk Assessment: Risk-based approach should be applied to decision making regarding the set-up of sanctions screening programme and this needs to be clearly documented.
   (iv) Internal controls: It is necessary to document how the screening system is configured in order to demonstrate that it is reasonably expected to manage specific sanctions risk.
   During the execution of his duties and the control of the compliance of the Financial Organisation with the Law and the present Directive, the compliance officer obtains and utilizes data, information and reports issued by the relevant international organizations (i.e. FATF, MONEYVAL, CFSP, UN, IMOLIN, IMF).

6.3. Alternate MLCO

The Company, in the absence of the MLCO, should appoint an Alternate MLCO.

The Alternate MLCO should be responsible to perform the duties of the MLCO and to ensure the compliance of the Company with the Law and the Directive and meets the conditions for the appointment of an MLCO. The Company may delegate the operation of the Alternate MLCO external only if the assignment is made to an individual.

The Company should immediately notify CySEC of the designation of the MLCO, the Alternate MLCO and Assistant MLCO by submitting their name, position and contact details.

It should be noted that the provisions of subsection 6.3 of this Manual do not apply when the MLCO resigns from his position, since in such case the Company should appoint a new MLCO.

7. ANNUAL REPORT OF THE MLCO

7.1. General

The Annual Report of the MLCO is a significant tool for assessing the Company's level of compliance with its obligation laid down in the Law and the Directive.

The MLCO's Annual Report shall be prepared and be submitted to the Board for approval within two months from the end of each calendar year (i.e. the latest, by the end of February each year).

Following the Board's approval of the Annual Report, a copy of the Annual Report should be submitted to CySEC together with the Board's meeting minutes, within twenty (20) days from the end of the meeting, and no later than three (3) months from the end of each calendar year (i.e. the latest, by the end of March).

It is provided that the said minutes should include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures.

The Annual Report deals with issues relating to money laundering and terrorist financing during the year under review and includes, *inter alia*, the following:

(a) information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the Directive which took place during the year under review
(b) information on the inspections and reviews performed by the MLCO, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Company applies for the prevention of Money Laundering and Terrorist Financing. In this respect, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation
(c) the number of Internal Suspicion Reports submitted by Company personnel to the MLCO, according to point (e) of Section 6.2 of the Manual and possible comments/observations thereon
(d) the number of reports submitted by the MLCO to the Unit, according to point (g) of Section 6.2 of the Manual with information/details on the main reasons for suspicion and highlights of any particular trends
(e) information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues
(f) summary figures, on an annualised basis, of Clients' total cash deposit in EUR and other currencies in excess of the set limit of EUR 10.000 (together with comparative figures for the previous year) as reported in the monthly prevention statement of Section 8 of the Manual. Any comments on material changes observed compared with the previous year are also reported.
(g) information on the policy, measures, practices, procedures and controls applied by the Company in relation to high risk Clients as well as the number and country of origin of high risk Clients with whom a Business Relationship is established or an Occasional Transaction has been executed
(h) information on the systems and procedures applied by the Company for the ongoing monitoring of Client accounts and transactions, as and when applicable
(i) information on the measures taken for the compliance of branches and subsidiaries of the Company, if any, that operate in countries outside the EEA, with the requirements of the Directive in relation to Client identification, due diligence and

record keeping procedures and comments/information on the level of their compliance with the said requirements

(j) information on the training courses/seminars attended by the MLCO and any other educational material received

(k) information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants

(l) results of the assessment of the adequacy and effectiveness of staff training

(m) information on the recommended next year's training program

(n) information on the structure and staffing of the department of the MLCO as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against Money Laundering and Terrorist Financing

(o) an executive summary in respect to the key findings and weaknesses identified during the year under review.

7.2. Monthly Prevention Statement

The MLCO shall prepare and submit to CySEC, according to point (q) of Section 5.2 of the Manual, on a monthly basis, the CySEC Form MPS "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing", which includes details as regards the total cash deposits accepted by the Company, the Internal Suspicions Reports, and the MLCO's Reports to the Unit, according to points (e) and (g) in Section 5.2 of the Manual, respectively.

The aforementioned Form must be completed and submitted to CySEC within fifteen (15) days from the end of each month.

According to Circular C567, the duly completed and signed Form MPS should be submitted to CySEC only electronically via CySEC Transaction Reporting System.

The completion of the aforementioned Form provides the opportunity to the Company initially to evaluate and, subsequently, to reinforce its systems of control and monitoring of its operations, for the purpose of early identification of transactions in cash which may be unusual and/or carry enhanced risk of being involved in Money Laundering and Terrorist Financing operations.

The Internal Auditor shall be responsible to review, at least annually as per Section 4 of the Manual, the submission to CySEC of the "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing".

8. RISK-BASED APPROACH

8.1. General Policy

The Company shall apply adequate and appropriate measures, policies, controls and procedures, depending on its nature and size, by adopting a risk-based approach, in order to mitigate and effectively manage the risks of Money Laundering and Terrorist Financing so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher. The said measures, policies, controls and procedures shall be applied by the Company at the level of branches and majority-owned subsidiaries by the Company whether in a Member State or third country, where applicable.

The Company shall take appropriate measures to identify and assess the risks of Money Laundering and Terrorist Financing, taking into account risk factors including those relating to its Clients, countries or geographic areas, products, services, transactions or banking channels. Those measures should be proportionate to the size and nature of the Company.

The risk assessments referred above shall be documented, updated and made available to CySEC.

Further, the MLCO shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of Section 9 of the Manual.

The adopted risk-based approach that is followed by the Company, and described in the Manual, has the following general characteristics:

(a) recognises that the money laundering or terrorist financing threat varies across Clients, countries, services and financial instruments
(b) allows the Board to differentiate between Clients of the Company in a way that matches the risk of their particular business
(c) allows the Board to apply its own approach in the formulation of policies, procedures and controls in response to the Company's particular circumstances and characteristics
(d) helps to produce a more cost-effective system
(e) promotes the prioritisation of effort and actions of the Company in response to the likelihood of Money Laundering and Terrorist Financing occurring through the use of the Investment and Ancillary Services provided by the Company.

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 Money Laundering and Terrorist Financing risks faced by the Company.

Such measures include:

(a) identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, and geographical areas of operation of its Clients

(b) managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls

(c) continuously monitoring and improving the effective operation of the policies, procedures and controls

(d) performing identification and due diligence in accordance with the provisions of Sections 60-66 of the Law

(e) record keeping, in accordance with the provisions of Section 68 of the Law

(f) preparing the internal report and reporting to MOKAS in accordance with the provisions of Section 69 of the Law

(g) ensuring the existence of internal control, assessment and risk management in order to prevent Money Laundering and Terrorist Financing

(h) undertaking a thorough examination of any transactions which, by their very nature, are particularly susceptible of being linked to Money Laundering or Terrorist Financing offenses, and in particular of any complex or abnormally large transactions and of all the unusual transactions occurring without obvious economic or clear legitimate reason.

(i) setting up risk management practices

(j) setting up compliance management

(k) ensuring that sufficient recruitment policy is in place and assessment of the employees' integrity.

(l) Informing relevant employees in relation to:

- the systems and procedures in accordance with paragraphs (d) to (h) of this section
- the present Law
- the Directives issued by the competent Supervisory Authority according to Section 59(4) of the Law
- the European Union's Directives on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and
- the relevant requirements for personal data protection.

(m) performing ongoing training of their employees in the recognition and handling of transactions and activities which may be related to money laundering or terrorist financing

The Board of Directors shall assess and evaluate the risks it faces, for usage of the services provided for the purpose of money laundering or terrorist financing. The particular circumstances of the Company determine the suitable procedures and measures that need to be applied to counter and manage risks, the identification, recording and evaluation of risk that the Company faces presupposes the finding of the risk posed by the Company's Clients behaviour, the way the Client communicated with the Company and the risk posed by the services and financial instruments provided by the Client.

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 *inter alia* the following:

- the scale and complexity of the services offered
- geographical spread of the services, products 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 MLCO shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the MLCO shall also be responsible for the adequate implementation of the policies, procedures and controls on a risk-based approach. The Internal Auditor shall be responsible for reviewing the adequate implementation of a risk-based approach by the MLCO, at least annually, as per Section 5.1 of the Manual.

The Company when assessing the risk of money laundering and terrorist financing shall take into account, maong others, the Risk Factor Guidelines and any guidelines/guidance issued by the FATF.

8.2. Identification of Risks

8.2.1. General/Principles

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 Investment and Ancillary Services for the purpose of Money Laundering or Terrorist Financing. 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 Investment and Ancillary 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 CySEC that the extent of measures and control procedures it applies are proportionate to the risk it faces for the use of the Investment and Ancillary Services provided, for the purpose of Money Laundering and Terrorist Financing.

8.2.2. Company Risks

The following, *inter alia*, are sources of risks which the Company faces with respect to Money Laundering and Terrorist Financing:

(a) *Risks based on the Client's nature:*

- complexity of ownership structure of legal persons
- companies with bearer shares
- companies incorporated in offshore centres
- 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
- unwillingness of Client to provide information on the Beneficial Owners of a legal person
- Clients included in the leaked documents of Mossack Fonseca (Panama Papers)
- Clients convicted for a Prescribed Offence (and already served their sentence)
- is there a sound reason for changes in the client's ownership and control structure?
- Client's or Beneficial Owner's source of wealth or source of funds to be explained, through their occupation, inheritance or investments
- Clients with income and/or wealth from high risk sectors such as arms, construction, gambling and private military contractors.

(b) *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.
- Frequent changes to Client due diligence information or payment details
- Using multiple accounts without previous notification to the Company, especially when these accounts are held in multiple high-risk jurisdictions

- The Client's business, for example the customer's funds are derived from business in sectors that are associates with a high risk of financial crime
- Client request transactions that are complex, unusually, or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose
- Client's origin of wealth and/or source of funds cannot be easily verified
- Are there adverse media reports or other relevant sources of information about the client, for example are there any allegations of criminality or terrorism against the client or the beneficial owner?

(c) *Risks based on the Client's initial communication with the Company*:

- non face-to-face Clients
- Clients introduced by a third person.
- Does the Client use the products and services he/she has selected during the establishment of the business relationship with the Company?

(d) *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
- Financial arrangements involving jurisdictions associated with higher ML/TF risk
- Cross border arrangements where assets are deposited or managed in another financial institution, either of the same financial group or outside of the group, particularly where the other financial institution is based in a jurisdiction associated with higher ML/TF risk. The Company should pay particular attention to jurisdictions with higher levels of predicate offences, a weak AML/CTF regime or weak tax transparency standards
- To what extent are products or services cash intensive, as are many payment services but also certain current accounts?
  To what extent do products or services facilitate or encourage high-value transactions? Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes.

(e) *Geographical risk factors:*

- Countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems
- Countries identified by credible sources as having significant levels of corruption or other criminal activity

- Countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations
- Countries in which the Client and beneficial owner are based
- Countries that are the Client's and beneficial owner's main places of business
- Countries to which the Client and beneficial owner have relevant personal links
- Countries providing funding or support for terrorist activities or that have designated terrorist organisations operating within their country.

8.3. 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 Money Laundering and Terrorist Financing 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.

The risk assessment and the implementation of the measures and procedures result in the categorisation of Clients according to their risk appetite, in accordance with the Company's procedures as set out in Section 9.4 of this Manual. The categorisation is based on criteria which reflect the possible risk causes and each category is accompanied with the relevant due diligence procedures, regular monitoring and controls.

The Company shall prepare and maintain a Client list, which contain, inter alias, the Clients' names, account numbers, date of commencement of the business relationship and their risk classification. The respective list should be promptly updated with all new or existing Clients that the Company determined, in the light of additional information received, that fall under one of the risk categories.

In this respect, it is the duty of the MLCO 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 Sections 9 and 10 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.

8.4. Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the MLCO to undertake regular reviews of the characteristics of existing Clients, new Clients, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics or circumstances. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

8.5. Relevant International Organisations

The Company, when assessing the money laundering and terrorist financing risks and when applying *risk based* measures, should take into account, among others, the Risk Factor Guidelines and the Guidelines issued by the Financial Action Task Force (the "FATF").

For the development and implementation of appropriate measures and procedures on a risk based approach, and for the implementation of Client Identification and Due Diligence Procedures, the MLCO and the Head of the Administration/Back Office Department shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), country assessment reports] that are published in the following relevant international organisations:

(a) FATF - www.fatf-gafi.org
(b) The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (hereinafter "MONEYVAL") - www.coe.int/moneyval
(c) The EU Common Foreign & Security Policy (CFSP)- eeas.europa.eu/cfsp/
(d) The UN Security Council Sanctions Committees - www.un.org/sc/committees
(e) The International Money Laundering Information Network (IMOLIN) - www.imolin.org
(f) The International Monetary Fund (IMF) – www.imf.org.
(g) the Joint Committee European Supervisory Authorities - https://esas-joint-committee.europa.eu/
(h) the Ministry of Foreign Affairs regarding the United Nations Security Council Resolutions or Decisions (Sanctions) or/and the European Union Council Decisions and Regulations (Restrictive Measures) - http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument

the EU Sanctions Map - https://www.sanctionsmap.eu/#/main

9. CLIENT ACCEPTANCE POLICY

The Client Acceptance Policy (hereinafter the "**CAP**"), following the principles and guidelines described in this Manual, defines the criteria for accepting new Clients and defines the Client categorisation criteria which shall be followed by the Company and especially by the employees which shall be involved in the Client Account Opening process.

The MLCO shall be responsible for applying all the provisions of the CAP. In this respect, the Administration/Back Office Department together with the Compliance Department shall also be assisting the MLCO with the implementation of the CAP, as applicable.

The Internal Auditor shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually, as per Section 5 of the Manual.

9.1. General Principles of the CAP

The General Principles of the CAP are the following:

(a) the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client
(b) where the Client is a prospective Client, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set in Section 10 of the Manual
(c) all documents and data described in Section 10.5 of the Manual must be collected before and/or during accepting a new Client
(d) no account shall be opened in anonymous or fictitious names(s)
(e) no account shall be opened unless the prospective Client is approved by:
    - the Head of the Administration/Back Office Department
    - the MLCO or a person from the Company's compliance function

9.2. Criteria for Accepting New Clients (based on their respective risk)

This Section describes the criteria for accepting new Clients based on their risk categorisation.

9.2.1. Low Risk Clients

The Company shall accept Clients who are categorised as low risk Clients as long as the general principles under Section 9.1 are followed

Moreover, the Company shall follow the *Simplified Client Identification and Due Diligence Procedures* for low risk Clients, according to Section 10.7 of the Manual.

9.2.2. Normal Risk Clients

The Company shall accept Clients who are categorised as normal risk Clients as long as the general principles under Section 9.1 of the Manual are followed.

9.2.3. High Risk Clients

The Company shall accept Clients who are categorised as high risk Clients as long as the general principles under Section 9.1 of the Manual are followed.

Moreover, the Company shall apply the *Enhanced Client Identification and Due Diligence* measures for high risk Clients, according to Section 10.8 of the Manual as well as apply the due diligence and identification procedures for the specific types of high risk Clients mentioned in Section 10.8 of the Manual, as applicable.

9.3. Not Acceptable Clients

The following list predetermines the type of Clients who are not acceptable for establishing a Business Relationship or an execution of an Occasional Transaction with the Company:

- Clients who fail or refuse to submit, the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification
- Shell Banks (The Company is prohibited from entering into, or continuing, a correspondent relationship with a shell bank. The Company shall take appropriate measures to ensure that it does not engage in or continue correspondent relationships with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank).
- Credit institutions, financial organisations and legal persons that operate in the areas of the Republic under Turkish military occupation, which are not incorporated according to the laws of the Republic of Cyprus and do not possess operating licence for providing services from CySEC or any other relevant regulatory authority of the Republic of Cyprus, in view of Circular CI144-2008-11.
- Clients convicted for a Predicate Offence (and are yet to serve their sentence). Depending on the nature of Predicate Offence, is at the Company's discretion not to accept a Client even after having served his/her sentence.
- Clients included in Sanction Lists based on decisions of competent authorities of European Union, OFAC or other international organizations.
- Clients residing in third countries and jurisdictions where the Company is not legally allowed to provide its services.
- Clients that the Company's Payment System Providers have issued Risk Alerts and the MLCO after examining their data still considers them as *high risk*.
- Any persons included in the List of Specially Designated Nationals and Blocked Persons maintained by OFAC and any Persons who reside in jurisdictions where the Company, at its sole discretion, does not offer its services, including without limitation, the United States of America, as well as countries in respect of which OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals.
- Clients from Belgium.

- Clients where the MLCO exercised discretion and deemed them as unacceptable.

9.4. Client Categorisation Factors

This Section defines the criteria for the categorisation of Clients based on their risk. The MLCO shall be responsible for categorising Clients in one of the three (3) categories listed in 10.4.1-10.3 based on the criteria of each category. Note that fulfilling one or a combination of the criteria listed under each risk category shall not (unless explicitly stated) determine the AML risk classification of an individual Client. The Company shall consider Clients holistically in assessing their AML risk (and apply the corresponding due diligence scrutiny).

In this context the Company shall employ tools including an internally developed AML Risk Scoring Matrix taking into account:

- The European Banking Authority (EBA) published, on the 16th of December 2021, its final guidelines (EBA/GL/2021/16) on the characteristics of a risk-based approach to anti-money laundering and terrorist financing (**"AML/TF"**) supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis under Article 48(10) of Directive (EU) 2015/8491 (the **"Risk-Based Supervision Guidelines"**)
- Paragraph 12 of the Directive on simplified and enhanced Client due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions.

The Company shall score all potential clients using the Risk Scoring Matrix as part of its process of assessing their risks of money laundering and terrorist financing.

This Section defines the criteria for the categorisation of Clients based on their risk. The MLCO shall be responsible for categorising Clients in one of the following three (3) categories based on the criteria of each category set below:

9.4.1. Low Risk Clients

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk as referred to in Annex II and Article 63 of the Law:

(1) Client risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership

(b) public administrations or enterprises

(c) Client that are resident in geographical areas of lower risk as set out in point (3) below

(2) Product, service, transaction or delivery channel risk factors:

(a) Life insurance policies for which the premium is low

(b) Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme

(d) Financial products or services that provide appropriately defined and limited services to certain types of Clients, so as to increase access for financial inclusion purposes

(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money)

(3) Geographical risk factors:

(a) Member States

(b) third countries having effective AML/CFT systems

(c) third countries identified by credible sources as having a low level of corruption or other criminal activity

(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

The following types of Clients can be classified as low risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces provided that the risk for money laundering and terrorist financing is low and there is no suspicion for legitimating income from illegal revenue or terrorism financing:

- credit or financial institution covered by the EU Directive
- credit or financial institution carrying out one or more of the financial business activities as these are defined by the Law and which is situated in a country outside the EEA, which:
  - imposes requirements equivalent to those laid down by the EU Directive and
  - it is under supervision for compliance with those requirements
- listed companies whose securities are admitted to trading on a Regulated Market in a country of the EEA or in a third country which is subject to disclosure requirements consistent with community legislation
- domestic public authorities of countries of the EEA.

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 MLCO shall be responsible to gather the said information.

It is also provided that in the cases mentioned above, the Company may not ascertain the identity of the Client or the ultimate beneficial owner and may not collect information about the reason of the establishment and the intended nature of the business relationship before or after the establishment of the business relationship or the execution of an occasional transaction.

The said information shall be duly documented and filed, as applicable, according to the recording keeping procedures described in Section 14.1.

Finally, the Company shall monitoring on ongoing basis the transactions of low risk Clients to ensure that there are no suspicious transactions.

9.4.2. Normal Risk Client Factors

The following types of Clients can be classified as normal risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

- any Client who does not fall under the 'low risk Clients' or 'high risk Clients' categories set in Sections 9.4.1 and 9.4.3, respectively.

9.4.3. High Risk Client Factors

The following is a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in Annex III and Article 64 of the Law:

(1) <u>Client risk factors:</u>

(a) the business relationship is conducted in unusual circumstances;
(b) Clients that are resident in geographical areas of higher risk as set out in point (3);
(c) legal persons or arrangements that are personal asset-holding vehicles;
(d) companies that have nominee shareholders or shares in bearer form;
(e) businesses that are cash-intensive;
(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
(g) politically Exposed persons
(h) Clients included in the leaked documents of Mossack Fonseca (Panama Papers)
(i) Clients convicted for a Prescribed Offence (and already served their sentence)
(j) unwillingness of Client to provide information on the Beneficial Owners of a legal person.
(k) trust accounts
(l) "Clients accounts" in the name of a third person
(m) Clients who are involved in electronic gambling/gaming activities through the internet
(n) Clients from countries which inadequately apply FATF's recommendations

(o) any other Clients that their nature entail a higher risk of money laundering or terrorist financing

(p) Third country nationals who apply for residence rights or citizenship in a Member State in exchange of capital transfers, purchase of property or government bonds, or investment in corporate entities in that Member State.

(q) any other Client determined by the Company itself to be classified as such.

(2) <u>Product, service, transaction or delivery channel risk factors:</u>

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;

(d) payment received from unknown or non-associated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

(3) <u>Geographical risk factors:</u>

(a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;

(c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

(d) Countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country. 5.6.2015 L 141/115 Official Journal of the European Union EN.

(4) <u>Risk based on the Client's behaviour:</u>

(a) Client transactions where there is no apparent legal financial/commercial rationale

(b) situations where the origin of wealth and/or source of funds cannot be easily verified

(c) unwillingness of Clients to provide information on the Beneficial Owners of a legal person.

(5) <u>Risk based on the Client's initial communication with the Company:</u>

(a) non-face-to-face Client

(b) Clients introduced by a third person.

(6) <u>Risk based on the Company's services and financial instruments:</u>

(a) services that allow payments to third persons/parties

(b) large cash deposits or withdrawals

(c) products or transactions which may favour anonymity.

The following *inter alia* types of Clients and in line with the provisions as specified in Annex III of the Law, may be classified as *high risk* Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces:

- Clients who are not physically present for identification purposes (non face-to-face Clients)
- Clients whose own shares or those of their parent companies (if any) have been issued in bearer form
- 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 or High Risk Third Countries
- cross-frontier correspondent banking relationships with credit institutions-Clients from third countries
- any other Clients that their nature entail a higher risk of money laundering or terrorist financing
- any other Client determined by the Company itself to be classified as such.

10. CLIENT IDENTIFICATION AND DUE DILIGENCE PROCEDURES

10.1. Cases for the Application of Client Identification and Due Diligence Procedures

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

   (a) when establishing a Business Relationship
   (b) when carrying out Occasional Transaction that
      i. amounts to EUR 15.000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked
      ii. constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament exceeding EUR 1.000.
   (c) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction in the provision of the relevant Investment and Ancillary Services.
   (d) when there are doubts about the veracity or adequacy of previously Client identification data.
   (e) in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10.000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

(f) for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2.000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked.

(g) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction in the provision of the relevant Investment and Ancillary Service.

(h) when there are doubts about the veracity or adequacy of previously Client identification data.

In this respect, it is the duty of the MLCO to apply all the relevant Client Due Diligence Identification Procedures described in Section 10 of the Manual and the Company's Client Acceptance Policy, as applicable. Furthermore, the Head of Administration/Back Office Department shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in Section 14.1 of the Manual.

2. Client Identification and Due Diligence procedures include the following:

i. The identification of the Client and the verification of the identity of the Client on the basis of documents, data or information issued or obtained from a reliable and independent source:

- Creation of an economic profile for the Client/beneficial owner,
- Carrying out a suitability test for the Client/beneficial owner in accordance with article 26(2)(a) of the Investment Services and Activities and Regulated Markets Law (L.87(I)/2017), as this has been amended from time to time
- Carrying out an appropriateness test in accordance with Section 26(3)(2) of the Investment Services and Activities and Regulated Markets Law (L.87(I)/2017), as this has been amended from time to time.

It is noted that the carrying out of an appropriateness test/suitability test shall be performed in case the Company provides the MiFID services (i.e. portfolio management, investment advice or reception & transmission of orders) to *retail Clients*. Professional Clients shall be exempted from this step as the Company may assume that they have necessary knowledge and experience to understand the risk arising from the proposed investment.

ii. The identification of the beneficial owners' identity and taking reasonable steps to verify his/her identity in order to ensure that the Company is satisfied that it knows the beneficial owner. With regards to legal persons, trusts, companies, foundations and similar legal arrangements, reasonable steps should be taken to understand the structure of the ownership and Client control.

iii. The assessment and, where appropriate, the collection of information on the purpose and intended nature of the business relationship

iv. Continuous supervision of the business relationship by scrutinizing the transactions carried out during that relationship in order to ensure that the transactions carried out are consistent with the data and information held by the Company in relation to the Client, the business and the Client's risk profile, and, where necessary, with regards to the origin of the funds and ensuring that updated documents, data or information are kept.

Provided that when applying the measures of paragraphs (i) and (ii) above, the Company should verify that any third person who intends to act on behalf of the Client is duly authorized by the Client for that purpose and identifies and verifies the identity of the third party.

3. The Company being an Obliged Entity shall apply each of the Client due diligence measures and identification procedures as these have been set out above, but may determine the extent of such measures depending on the degree of risk taking into consideration at least the provisions of Annex I of the Law.

4. The Company must be able to demonstrate to the competent Supervisory Authorities that the extent of the measures is proportionate to the risks of Money Laundering and Terrorist Financing that is exposed to.

In this respect, it is the duty of the MLCO to apply all the relevant Client Due Diligence Identification Procedures described in Section 10 of the Manual for the cases mentioned above. Furthermore, the Head of Administration/Back Office Department shall also be responsible to collect and file the relevant Client identification documents, according to the recording keeping procedures described in Section 14.1 of the Manual.

Further, the MLCO 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 Law and the Directive.

The Internal Auditor shall be responsible to review the adequate implementation of all the policies and procedures mentioned in Section 10 of the Manual, at least annually, as per Section 5 of the Manual.

The Company is using Refinitiv World Check for the onboarding and ongoing customer screening. Refinitiv World Check service provider is to aid in the automated screening of clients, in order to detect and assess whether the client is subject to EU/UN and international sanctions (Clients are screened on more than 150 sanction lists), politically exposed person (PEP), convicted or suspected criminal.

The Company ensures that the screening system is appropriate to the nature, size and ML/TF risks the obliged entity is exposed of the Company. Screening is performed on clients before: performed before:

- the establishment of a business relationship;

- the provision of any services; and
- undertaking any transactions for a customer.

Thereafter, monitoring is undertaken on an ongoing basis for customers and customers' related entities, directors, and beneficial owners.

Further to this the Company ensures:

- that customer data used for ongoing screening is up to date and correct
- that there is a full understanding of the capabilities and limits of the automated screening system
- that the automated screening system can be tailored in line with the Company's' risk appetite and perform regular reviews of the calibration and rules to ensure its effective operation.

The Company has implemented controls that require referral to the MLCO prior to dealing with flagged persons.

Upon identification of a match through Refinitiv World Check, the Compliance Department's staff investigate the potential match to ascertain if it is an actual match to the client or if it is a false positive. If a potential match is found, Compliance Department refer to the MLCO for further direction.

The MLCO will:

- notify *Senior Management*,
- freeze/disconnect accounts where appropriate and where an actual target match is identified,
- keep a clear, documented audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive.

10.2. Transactions that Favour Anonymity

In the case of Clients' transactions via internet, phone, fax or other electronic means where the Client is not present so as to verify the authenticity of his signature or that he is the real owner of the account or that he has been properly authorised to operate the account, the Company applies reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it deals with the true owner or the authorised signatory of the account.

10.3. Failure or Refusal to Submit Information for the Verification of Clients' Identity

Failure or refusal by a Client to submit, before or during the establishment of a Business Relationship or the execution of an occasional transaction, the requisite data and information for the verification of his identity and the creation of his economic profile (see Section 10.5 of

the Manual), without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Client is involved in money laundering or terrorist financing activities. In such an event, the Company shall not proceed with the establishment of the Business Relationship or the execution of the occasional transaction while at the same time the MLCO considers whether it is justified under the circumstances to submit a report to the Unit, according to point (g) of Section 6.2 of the Manual.

If, before or during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe, the required verification data and information according to Section 10 of the Manual, the Company and the MLCO shall terminate the Business Relationship and close all the accounts of the Client, taking also into account the specific circumstances of the Client in question and the risks faced by the Company on possible money laundering and/or terrorist financing, while at the same time examine whether it is justified under the circumstances to submit a report to Unit, according to paragraph point (g) of Section 6.2 of the Manual.

10.4. Time of Application of the Due Diligence and Client Identification Procedures

10.4.1. General

With respect to the extent that the Company shall apply Client due diligence measures, the MLCO shall be responsible for the consideration of the following, non-exhaustive list, of risk variables:

(i) the purpose of an account or relationship,
(ii) the level of assets to be deposited by a Client or the size of transactions undertaken,
(iii) the regularity or duration of the business relationship.

With respect to the timing of the application of the Due Diligence and Client Identification Procedures, the MLCO shall be responsible for the application of the following provisions:

1. The verification of the identity of the Client and the Beneficial Owner shall be performed before the establishment of a Business Relationship or the carrying out of a transaction.

2. By way of derogation from point (1) above, the verification of the identity of the Client and the Beneficial Owner may be completed during the establishment of a Business Relationship if this is necessary not to interrupt the normal conduct of business, where the risk of money laundering or terrorist financing occurring is *low* in such situations, the process of verifying the procedure is completed as soon as possible after the initial contact.

3. By way of derogation from point (1) above, the Company may allow the opening of an account with a credit institution or financial institution, including accounts that permit transactions in transferable securities, provided that these are adequate safeguards in place to ensure that transactions are not carried out by the Client or on its behalf until full compliance with the Client due diligence requirements laid down in Section 10.1 above.

4. In cases where the Company is unable to comply with Subsections (a), (b) and (c) of Section 61 of the Law, it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall terminate the business relationship and consider making a suspicious transaction report to the Unit, in relation to the Client, in accordance with the provisions of Section 69.

5. Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing (see points (b) to (d) of Section 10.1 of the Manual) including at times when the relevant circumstances of a Client change.

6. Without prejudice of what is stated in point (2) above by way of derogation from point (1) above, for cases that fall under the supervision of CySEC the verification of the identity of the Client and the beneficial owner may be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring and the process of verification is completed as soon as practicable after the initial contact.

7. In applying the measures referred to in paragraphs (a) and (b) above, the Company shall verify that any third party intending to act on behalf of its Client is duly authorized by the Client for that purpose and should identify and verify the identity of this person.

8. In accordance with Section 61(2) of the Law, Obliged Entities shall apply the Client identification procedures and Client due diligence measures referred to in Section 61 (1) of the Law but may determine the extent of such measures according to the degree of risk taking into account at least the following variables (as per Annex I of the Law and as stated below):
    - the purpose of an account or relationship
    - the level of assets to be deposited by a Client or the size of transactions undertaken
    - the regularity or duration of the business relationship.

9. In accordance with Section 61(3) of the Law for the purposes of the provisions on identification methods and customer due diligence measures, proof of identity is sufficient if:
    - It is reasonable to ensure that the Client is indeed the person who claims to be and

- the person examining the evidence of the Client is satisfied, that the Client is in fact the person who claims to be.

10. In cases where the Company is unable to comply with subsections (a), (b) and (c) of Section 61 of the Law, it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, and shall terminate the business relationship and consider making a suspicious transaction report to the Unit, in relation to the Client.

11. Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing (see points (b) to (d) of Section 10.1 of the Manual) including at times when the relevant circumstances of a Client change.

10.4.2. Verification of Client's identity during the establishment of a business relationship (Extraordinary Cases when the risk is assessed as *low*)

Further to point (3) of Section 10.4.1 of this Manual, the Company when commencing the establishment of a business relationship with a Client whose identity has not yet been verified, the risk may be assessed as low when, at a minimum, the following, among others, are taken into consideration:

(a) In cases where the verification of the identity of the Client/beneficial owner has not yet been completed, the cumulative amount of deposited funds of a Client should not exceed EUR 2.000, irrespective of the number of accounts the Client holds with the Company. The amount of EUR 2.000 shall not automatically categorise the Client as *low risk*.
(b) The Company shall accept deposits only from a bank account (or through other means that are linked to a bank account (e.g. credit card), that is in the name of the Client with whom establishes a business relationship.
(c) The cumulative amount of time in which the verification of the identity of the Client is completed, must not exceed fifteen (15) days from the initial contact.
(d) It is noted that the initial contact takes place the moment that the Client either accepts the terms and conditions or makes his first deposit, whichever comes first.
(e) Further to the above, within the timeframe of fifteen (15) days from the initial contact, the Company shall take all reasonable measures to ensure that the percentage of Clients that have not complied with the request to submit verification documents is considerably low. Such measures may include, *inter alia*, the sending of reminders and/or requests to Clients informing them of their obligation to submit the requested documents for the completion of the verification of their identity.
(f) Where the verification of the Client's identity has not been completed during the designated timeframe of fifteen (15) days, the commencement of the business relationship must be terminated on the date of the deadline's expiry and all deposited funds must be returned automatically to the Client, and in the same bank account from

which they originated, with such return to be done immediately, regardless of whether the Client has requested the return of their funds or not.

Note: the returned funds (deposits) include any profits the Client has gained during their transactions and exclude any losses incurred.

(g) Within the timeframe of fifteen (15) days from the initial contact, the Client should undergo at least one (1) Enhanced Due Diligence measure in accordance to Section 10.8 of this Manual.

Further to the above and excluding the cases of suspicion of money laundering, where the Company is under an obligation to immediately report their suspicion to the Unit and notify CySEC of the suspicious transaction incident, no funds will be held and no accounts will be frozen by the Company (see also Section 6.2 of this Manual).

Conducting transactions with a Client, during the establishment of a business relationship may occur, in cases where the conditions in paragraph 2 above apply.

The Company will not accept deposits, where the Client has not provided information as to:

(a) the full identification and
(b) the creation of their economic profile in accordance to Section 10.5 of this Manual, and
(c) the completion of their suitability test and/or
(d) the completion of their appropriateness test.

In cases where the Company is unable to comply with points (a) to (c) of Section 9.1 of the Manual, the Company shall not carry out a transaction through a bank account, establish a Business Relationship or carry out the transaction, or must terminate the business relationship and shall consider making a report to the Unit.

Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times (see points (b) to (d) of Section 9.1 of the Manual), depending on the level of risk of being involved in money laundering or terrorist financing (see points (b) to (d) of Section 9.1 of the Manual).

10.5. Construction of an Economic Profile and General Client Identification and Due Diligence Principles

1. The construction of the Client's economic profile needs to include/follow the principles below:

(a) the Company shall be satisfied that it's dealing with a real person and, for this reason, the Company shall obtain sufficient evidence of identity to verify that the

person is who he claims to be. Furthermore, the Company shall verify the identity of the Beneficial Owner(s) of the Clients' accounts. In the cases of legal persons, the Company shall obtain adequate data and information so as to understand the ownership and control structure of the Client. Irrespective of the Client type (e.g. natural or legal person, sole trader or partnership), the Company shall request and obtain sufficient data and information regarding the Client business activities and the expected pattern and level of transactions. However, it is noted that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative

(b) the verification of the Clients' identification shall be based on reliable data and information issued or obtained from independent and reliable sources, meaning those data, and information that are the most difficult to be amended or obtained illicitly

(c) a person's residential and business address will be an essential part of his identity

(d) the Company will never use the same verification data or information for verifying the Client's identity and verifying its home address

(e) the data and information that are collected before or during the establishment of the Business Relationship, with the aim of constructing the Client's economic profile and, as a minimum, shall include the following:

- the purpose and the reason for requesting the establishment of a Business Relationship
- the anticipated account turnover, the nature of the transactions, the expected origin of incoming funds to be credited in the account and the expected destination of outgoing transfers/payments
- the Client's size of wealth and annual income and the clear description of the main business/professional activities/operations

(f) the data and information that are used for the construction of the Client-legal person's economic profile shall include, *inter alia*, the following:

- the name of the company
- the country of its incorporation
- the head offices address
- the names and the identification information of the Beneficial Owners
- the names and the identification information of the directors
- the names and the identification information of the authorised signatories
- financial information
- the ownership structure of the group that the Client-legal person may be a part of (country of incorporation of the parent company, subsidiary companies and associate companies, main activities and financial information).

The said data and information are recorded in a separate form designed for this purpose which is retained in the Client's file along with all other documents as well as all internal records of meetings with the respective Client. The said form is updated regularly or whenever new information emerges that needs to be added to

the economic profile of the Client or alters existing information that makes up the economic profile of the Client.

(g) identical data and information with the abovementioned shall be obtained in the case of a Client-natural person, and in general, the same procedures with the abovementioned shall be followed

(h) Client transactions transmitted for execution, shall be compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Client and the data and information kept for the Client's economic profile. Significant deviations are investigated and the findings are recorded in the respective Client's file. Transactions that are not justified by the available information on the Client, are thoroughly examined so as to determine whether suspicions over money laundering or terrorist financing arise for the purposes of submitting an internal report to the MLCO, according to point (e) of Section 6.2 of the Manual, and then by the latter to the Unit, according to point (g) of Section 6.2 of the Manual.

2. The Company shall apply each of the Client due diligence measures and identification procedures set out in point (1) 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. The Company shall be able to demonstrate to CySEC that the extent of the measures is appropriate in view of the risks of the use of the Investment and Ancillary Services for the purposes of Money Laundering and Terrorist Financing.

3. For the purposes of the provisions relating to identification procedures and Client due diligence requirements, proof of identity is satisfactory if-

   (a) it is reasonable possible to establish that the Client is the person he claims to be, and,

   (b) the person who examines the evidence is satisfied, in accordance with the procedures followed under this Law, that the Client is actually the person he claims to be.

The construction of the Client's economic profile according to the provisions above shall be undertaken by the MLCO. In this respect, the data and information collected for the construction of the economic profile shall be fully documented and filed, as applicable, by the Head of the Administration/Back Office Department.

10.6. Further Obligations for Client Identifications and Due Diligence Procedures

1. In addition to the principles described in Section 10.5. above, the Company, and specifically the MLCO shall:

(a) ensure that the Client identification records remain completely updated with all relevant identification data and information throughout the Business Relationship
(b) examine and check, on a regular basis, the validity and adequacy of the Client identification data and information that he maintains, especially those concerning high risk Clients.

The procedures and controls of point (a) in Section 6.2 of the Manual also determine implicit the timeframe during which the regular review, examination and update of the Client identification is conducted. The outcome of the said review shall be recorded in a separate note/form which shall be kept in the respective Client file.

2. Despite the obligation described in point (1) above and while taking into consideration the level of risk, if at any time during the Business Relationship, the Company becomes aware that reliable or adequate data and information are missing from the identity and the economic profile of the Client, then the Company takes all necessary action, by applying the Client identification and due diligence procedures according to the Manual, to collect the missing data and information, the soonest possible, so as to identify the Client and update and complete the Client's economic profile.

   If, during the Business Relationship, a Client fails or refuses to submit, within a reasonable timeframe the required verification data and information, the Company shall terminate the Business Relationship and closes all the accounts of the Client while at the same time shall examine whether it is justified under the circumstances to submit a report to the Unit, according to point (g) of Section 6.2 of the Manual.

3. In addition to the obligation of points (1) and (2) above, the Company shall check the adequacy of the data and information of the Client's identity and economic profile, whenever one of the following events or incidents occurs:

   (a) an important transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the economic profile of the Client
   (b) a material change in the Client's legal status and situation, such as:
      i. change of directors/secretary
      ii. change of registered shareholders and/or Beneficial Owners
      iii. change of registered office
      iv. change of trustees
      v. change of corporate name and/or trading name
      vi. change of the principal trading partners and/or undertaking of major new business activities
   (c) a material change in the way and the rules the Client's account operates, such as:
      i. change in the persons that are authorised to operate the account
      ii. application for the opening of a new account for the provision of new investment services and/or financial instruments.

4. In addition to the above, the Company, when making transfers of money between Clients' accounts, shall apply the following procedures in accordance to Circular CI144-2012-09, as applicable:

   (a) Ask, from both Clients directly involved (originator of the transfer and recipient of the transfer), to complete a form of order and acceptance of the money transfer between the Clients' accounts.

   (b) Before performing the money transfer, the responsible, for this purpose, person (e.g. Head of the Accounting Department) shall confirm the order and acceptance of the money transfer by telephone or by other equivalent method. If the confirmation is made by telephone, the telephone communication shall be recorded.

   (c) The MLCO shall:

      i. verify the authenticity of the signatures on the aforementioned form

      ii. record (e.g. on the form) the reasons and confirm the legality of the purpose for which the transfer of money is made

      iii. keep/file all records and information related to this purpose in the involved Clients' files.

10.7. Simplified Client Identification and Due Diligence Procedures

With respect to the provisions of the Law and the Directive for simplified Client Identification and Due Diligence Procedures, the following shall apply:

1. The Company may apply simplified Client due diligence measures if they are previously satisfied that the business relationship or transaction has a lower degree of risk.

   The Company shall be adequately monitoring the relevant transactions and the business relationship, so that unusual or suspicious transactions can be traced.

2. When assessing the risks of Money Laundering and Terrorist Financing related to Client categories, geographic areas and to specific products, services, transactions or delivery/service channels, the Company shall take into account at least the factors relating to the situations of potentially lower risk, as specified in Annex II of the Law.
   By way of derogation from Sections 10.1 and 10.4 of the Manual and on the basis of an appropriate risk assessment showing that the risk of Money Laundering and Terrorist Financing is low, the Company may not apply certain Client due diligence measures in respect of electronic money if all of the following risk mitigation conditions are met:

   (a) The payment instrument is not reloadable or has a maximum monthly payment transaction limit of EUR 150 that can be used for payment transactions only within the Republic,
   (b) The maximum amount stored electronically does not exceed EUR 150,
   (c) The payment instrument is used exclusively for the purchase of goods or services,
   (d) The payment instrument cannot be funded with anonymous electronic money,

(e) The issuer has adequate and sufficient systems and procedures to monitor transactions or business relationships in order to detect unusual or suspicious transactions.

However, the above provisions of shall not apply in case there is a cash repayment or cash withdrawal of the monetary value of the electronic money and the amount exceeds EUR 50. Furthermore, the obligation to monitor on an on-going basis the transactions and the business relationship as well as detecting and reporting any suspicious transactions is not waived.

With respect to public authorities or public bodies of the EEA countries, for which the provisions of point (1) of Section 10.5 may not be applied, they must fulfil all the following criteria:

a. the Client has been entrusted with public functions pursuant to the Treaty on European Union, the Treaties on the Communities or Community secondary legislation
b. the Client's identity is publicly available, transparent, and certain
c. the activities of the Client, as well as its accounting practices, are transparent

either the Client is accountable to a community institution or to the authorities of a member state, or appropriate check and balance procedures exist ensuring control of the Client's activity.

10.8. Enhanced Client Identification and Due Diligence (High Risk Clients)

10.8.1. General Provisions

The MLCO shall apply enhanced due diligence measures, in addition to the measures referred to in Sections 10.1, 10.4, 10.5 and 10.6, with respect to the Clients categorised as high risk Clients according to the criteria set in Section 9.4.3 of this Manual.

These measures include the following:

(a) Where the Client has not been physically present for identification purposes, the Company shall apply one or more of the following measures:
    i. take supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution
    ii. ensure that the first payment of the operations is carried out through an account opened in the Client's name with a credit institution which operates in a country within the EEA.
    iii. Direct confirmation of the client's business relationship with a credit or financial institution which operates, and it is licensed in a country within the EEA or a 3rd country, which it is assessed by the Company as lower risk 3rd country, taking into consideration Annex II of the Law and the Guidelines. The said confirmation should be obtained through the Company's direct contact

with the said credit or financial information, and it should contain the client's true name, residential address and passport/ID number.

iv. Telephone contact with the client (in the case of a natural person) at his home or office and in the case of a legal person, at its head office address, on a telephone number that has been verified from independent and reliable source. During the telephone contact, the Company should confirm additional aspects of the identity information which were submitted by the client during the procedure of opening his/its account with the Company.

v. Communication with the Client through an address that the Company has previously verified from independent and reliable sources, in the form of a registered letter (for example, such communication may take the form of a direct mailing of account opening documentation to him, which the client shall return to the Company or the Company may send security codes required by the client to access the online account he opened with the Company).

(b) Where the Company transacts with a natural person or legal entity with an establishment in a high-risk third country, it is provided that enhanced Client due diligence measures need not be automatically invoked with respect to branches or majority owned subsidiaries of the Company established in the European Union which are located in high risk third countries, where those branches or majority owned subsidiaries fully comply with the group-wide policies and procedures in accordance with the provisions of section 68A of the Law and, in such a case, the Company will use the risk-based approach.

(c) In respect of cross-frontier correspondent banking relationships with credit/financial institutions-Clients from third countries, the Company shall:

i. gather sufficient information about the credit/financial institution-Client to understand fully the nature of the business and the activities of the Client and to assess, from publicly available information, the reputation of the institution and the quality of its supervision

ii. assess the systems and procedures applied by the credit/financial institution-Client for the prevention of Money Laundering and Terrorist Financing

iii. obtain approval from the *Senior Management* before entering into correspondent bank account relationships

iv. document the respective responsibilities of the person engaged in financial or Other Business Activities and of the credit/financial institution-Client

v. with respect to payable-through accounts, must be ensured that the credit institution-Client has verified the identity of its Clients and performed ongoing due diligence on the Clients having direct access to the correspondent bank accounts and that it is able to provide relevant Client's due diligence data to the correspondent institution, upon request.

(d) With respect to transactions or Business Relationships with a PEP, or a immediate family member of a close associate of a PEP, as applicable, the Company shall:

i. have appropriate risk-based procedures to determine whether the Client or the ultimate beneficial owner is a PEP
ii. have *Senior Management* approval for establishing Business Relationships with such Clients or for continuation of the business relationships with existing Clients who are either PEPs or have become PEPs.
iii. take adequate measures to establish the source of wealth and source of funds in relation to such persons
iv. carry out increased and continuous monitoring of these business relationships,
v. provided that when a PEP has ceased to be entrusted with a prominent public function/office in the Republic or in a Member State or in a third country, or ceased to hold a prominent public position in an international organization, the Company shall take into consideration, for a period of at least twelve (12) months, the risk that the person continues to pose and it shall apply the appropriate measures, depending on the degree of risk, until it is considered that the person no longer has a particular risk which characterizes him/her as a PEP
vi. apply to the close relatives or persons known to be close associates of a PEP, the measures referred to in points (i) to (v) above.

The Company shall take reasonable steps to determine whether the beneficiaries of a life insurance policy or other insurance policy with investment purpose and/or, where appropriate, the beneficial owner of the beneficiary are PEPs. Such measures shall be taken at the latest when the product of the insurance contract is paid or at the time of the whole or part of the insurance contract.

Where (i) the policyholders of a life insurance policy or other insurance policy with the investment objective and/or, where applicable, the beneficial owner of the beneficiary, is defined as PEP at the time of payment of the product of the insurance contract or at the time of the assignment, and/or (ii) where higher risks are identified in transactions or business relationships with PEPs, in addition to the implementation of the Client due diligence measures:

i. Inform senior executives before payment of the product of the insurance policy,
ii. Carry out increased control of the entire business relationship with the counterparty.

(e) The Company shall apply enhanced Client due diligence measures, in addition to the measures referred to in Sections 60, 61 and 62 of the Law, and in other cases which by their nature pose a high risk of Money Laundering or Terrorist Financing. In assessing such risks, the entities under consideration shall at least take into account the potentially higher risk situations as specified in Annex III of the Law.

(f) The Company must examine, to the extent possible, the history and purpose of all complex and unusually large transactions, and all unusual types of transactions that are carried out without an obvious economic or legitimate purpose.

In particular, the Company shall increase the degree and nature of the business relationship monitoring in order to determine whether such transactions or activities appear to be suspicious.

Below are described due diligence and identification procedures with respect to high risk Clients:

10.8.2. Non face-to-face Clients

The MLCO shall apply the following with respect to non face-to-face Clients or transaction as specified in paragraph 2(c)of Appendix III of the Law, presents higher risk of money laundering or terrorist financing, it should apply enhanced customer due diligence measures. The said measures may be the following:

1. Whenever a Client requests the establishment of a business relationship or an occasional transaction, a personal interview is recommended during which all information for Client identification should be obtained In situations where a Client, especially a non-resident of the Republic, requests the establishment of a Business Relationship or an Occasional Transaction through mail, telephone, or the internet without presenting himself for a personal interview, the Company shall follow the established Client identification and due diligence procedures, as applied for Clients with whom it comes in direct and personal contact and obtain exactly the same identification information and documents, as required by the Law and the Directive, depending on the type of the Client. The said identification information and documents be kept by the Company in its records shall take the following form:
    i. Original, or
    ii. Certified true copy of the original, where the certification is made by the Company itself in cases where it establishes the Client's identity itself, once the original is presented thereto, or
    iii. Certified true copy of the original, where the certification is made by third parties, in cases where they establish the Client's identity, pursuant to Section 10.10 of this Manual, or
    iv. Certified True copy of the original, where the certification is made by a competent authority or person that pursuant of the legislation of their countries, is responsible to certify the authenticity of documents or information, in cases where they establish the Client's identity themselves. In this case, the documents should be apostilled or notarised, or or
    v. Copy of the original, provided that at least one of the procedures referred to paragraph 2 below is followed.

2. Further to the supplementary measures to verify supplied documents of a Client, who has not been physically present for identification purposes, referred to in Section 10.8.1 (a) (i) of this Manual, the Company may utilize the below practical procedures for obtaining additional documents, data or information for the verification of a Client's identity:
   i. The first payment of the operations is carried out through an account held in the Client's name with a credit institution operating and licensed in a third country, which has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the Company.
   ii. Obtaining an original or true copy of a direct confirmation of the establishment of a business relationship of a business relationship through direct personal contact, as well as the true name, address, and passport/identity card number of the Client, from a credit institution or a financial institution, with which the Client cooperates, operating in a Member States or a Third country which has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the Company.
   iii. Contacting the Client via a telephone call at his home or office, on a telephone number verified by an independent and reliable source, during which the Company shall confirm additional aspects of the identity information submitted by the Client during the Client account opening process,
   iv. Communicating the Client via a video conference call, provided the video recording and screen shot safeguards apply to such communication.

   It is provided that a Client, whose identity was verified hereunder cannot deposit an amount over EUR 2000 per annum, irrespective of the number of accounts that he/she keeps with the Company, unless the Company, for the verification of the Client's identity:

   (a) takes an additional measure, as per paragraph 2 above,
   (b) takes supplementary measures to verify or certify the documents supplied by the Client,
   (c) requires confirmatory certification by a credit or financial institution covered by the EU Directive, in relation to the Client.

   Further to the above, the Company shall apply appropriate measures and procedures in order to:

   1. Confirm and monitor both the amount of the Client's deposit and the risk for money laundering or terrorist financing, as well as to take additional measures to verify the Client's identity depending on the degree of the risk,
   2. Ensure the normal conduct of business is not interrupted where the amount of the Client's deposit exceeds the amount of EUR 2.000 annually,
   3. Warn the Client appropriately and in due time for the above mentioned procedure in order to obtain the Client's express consent, prior to its commencement

v. Communicating with the Client through at an address that the Company has previously verified from an independent and reliable source, in the form of registered letter e.g. direct mailing of account opening documentation, which the Client shall return to the Company or the sending of security codes required by the Client to access the accounts opened.

vi. Electronic identity verification is carried out either by the Company directly or by a third party, pursuant that both the Company and such third party satisfy the below conditions:

1. The electronic databases kept by the third party or which the third party or the Company has access are registered to and/or approved by the Data Protection Commissioner or the corresponding competent authority in the country the said databases are kept, in order to safeguard personal data,
2. Electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information, at least the Client's full name, address and date of birth, and negative information such as committing offences as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures' list by the Council of European Union and the UN Security Council,
3. Electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter,
4. Transparent procedures have been established allowing the Company to know which information was searched, the result of such search and its significance in relation to the level of assurance as to the Client's identity verification,
5. Procedures have been established allowing the Company to record and save the information used and the result in relation to identity verification.

In addition to the above, the Company evaluates the results of electronic verification in order to be satisfied that proof of identity has been carried out satisfactorily, in accordance to point 3 of Section 10.5 of this Manual.

The Company should always be in a position to establish mechanisms for the carrying of quality controls in order to assess the quality of information on which it intends to rely.

i. The Company should receive information for electronic verification at least from two or more sources and the electronic verification procedure shall at least satisfy the following conditions:

- Identification of the Client's full name and current address from one source, and
- Identification of the Client's full name and either his current address or date of birth from a second source

ii. Further to the above, the Company shall establish procedures in order to satisfy the completeness, validity and reliability of the information to which it has access, for the purposes of carrying out the electronic verification. It is provided that the verification procedure shall include a search of both positive and negative information.

iii. Use of Innovative methods, or a combination of them as per the CySEC's Consultation Paper CP-02-2020. Such methods may include without limitation identity verification by taking a dynamic real time selfie, and/or of a real time video call. The following conditions shall be meet be cumulatively fulfilled:

(i) The use of such methods take place on a risk-based approach depending on the level of assets to be deposited and the size of transactions involved.

(ii) A detailed assessment of the risks emanating from the use of such methods and of the measures employed to mitigate such risks has taken place in advance in accordance with of Part IV of the AML Directive, whereas such assessment is updated on an ongoing basis and it allows on a reasonable, consistent and demonstrable basis to conclude that the money laundering risks, including the risks of identity theft, impersonation and identity fraud, are sufficiently reduced.

(iii) Before the Company make use of such innovative methods, it shall inform CySEC in advance by defining the methods to be used and by submitting the standardized attestation.

(iv) The use of such innovative methods takes place in accordance with the relevant best practices and guidelines published by the CySEC.

(v) The Company must ensure that documentation, data and information gathered during the customer on-boarding process through innovative solutions remain accurate and up to date.

(vi) The Company shall be responsible to set an explicit limit on the level of assets to be deposited and the size of transactions involved in order to be able to use an innovative identification method. Such limit is expected to vary per risk category and on a case-by-case basis, depending on the particular risks involved and on whether a combination of Innovative CDD methods were used or were complemented with non-innovative/non-electronic CDD methods.

(vii) The persons within the Company that are responsible for the selection, including the documented justification in the risk assessment mentioned herein, implementation and monitoring of the Innovative Method(s), are the Board of Directors, the MLCO. The Internal Auditor will be responsible for independently auditing the risk assessment and the practical application of the selected Innovative Method(s) and where deficiencies are identified to be immediately rectified.

10.8.3. Account in names of companies whose shares are in bearer form

The MLCO shall apply the following with respect to accounts in names of companies whose shares are in bearer form:

1. The Company may accept a request for the establishment of a Business Relationship or for an Occasional Transaction from companies whose own shares or those of their parent companies (if any) have been issued in bearer form by applying, in addition to the procedures of Section 10.9.6, all the following supplementary due diligence measures:

(a) the Company takes physical custody of the bearer share certificates while the Business Relationship is maintained or obtains a confirmation from a bank operating in the Republic or a country of the EEA that it has under its own custody the bearer share certificates and, in case of transferring their ownership to another person, shall inform the Company accordingly

(b) the account is closely monitored throughout its operation. At least once a year, a review of the accounts' transactions and turnover is carried out and a note is prepared summarising the results of the review which shall be kept in the Client's file

(c) if the opening of the account has been recommended by a third person as defined in Section 10.10, at least once every year, the third person who has introduced the Client provides a written confirmation that the capital base and the shareholding structure of the company-Client or that of its holding company (if any) has not been altered by the issue of new bearer shares or the cancellation of existing ones. If the account has been opened directly by the company-Client, then the written confirmation is provided by the company-Client's directors

(d) when here is a change to the Beneficial Owners, the Company examines whether or not to permit the continuance of the account's operation.

10.8.4. Trust accounts

The MLCO shall apply the following with respect to trust accounts:

1. When the Company establishes a Business Relationship or carries out an Occasional Transaction with trusts, it shall ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and Beneficial Owners, according to the Client identification procedures prescribed in throughout Section 10 of this Manual. Nevertheless, the Company shall receive sufficient information about the beneficiary to ensure the Company is to be able to identify the beneficial owner at the time of the payment or when the beneficiary exercises his acquired rights.

2. Furthermore, the Company shall ascertain the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the trustees. All relevant data and information shall be recorded and kept in the Client's file.

3. The Company shall maintain a central register of beneficial owners of trusts when the trust generate tax consequences in the Republic of Cyprus. The said register must hold adequate, accurate and current information on their beneficial ownership, including the identity of:
    - the trustee,
    - the settlor,
    - the protector,
    - the beneficiaries or class of beneficiaries and
    - any other natural person exercising effective control over the trust.

The said register should be accessible, within the framework of their responsibilities, to (The Company will also have access to the beneficial owners in the framework of Client due diligence):

- CySEC,
- the Unit,
- the Department of Customs and Excise,
- the Tax Department and
- the Law Enforcement.

10.8.5. 'Client accounts' in the name of a third person

The MLCO shall apply the following with respect to "Client accounts" in the name of a third person:

1. The Company may open "Client accounts" (e.g. omnibus accounts) in the name of financial institutions from EEA countries or a third country which has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the Company. In these cases the Company shall ascertain the identity of the abovementioned financial institutions according to the Client identification procedures prescribed in throughout Section 10 of the Manual.

2. In case the Company receives a request to open "Client accounts" (e.g. omnibus accounts) in the name of financial institutions originating from countries other than the EEA or an equivalent third country, then the Company shall examine such requests on a case by case basis and shall undertake additional due diligence measures on such financial institutions. Such additional measures shall include a country-profile assessment in terms of AML reputation and legislation, analysis of the AML measures applied by such financial institutions, whether he financial institution is supervised in terms of AML, analysis of the line of business and Clientele type of the financial institution and any additional measures deemed necessary during the assessment. It is stressed that the Company shall be extra vigilant on such cases.

3. In the case that the opening of a "Client account" is requested by a third person acting as an auditor/accountant or an independent legal professional or a trust and company service provider situated in a country of the EEA or a third country which, in accordance with a relevant decision of the Advisory Authority it has been determined that the relevant third country applies procedures and measures for preventing money laundering and terrorist financing and has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the

Company itself, the Company shall proceed with the opening of the account provided that the following conditions are met:

(a) the third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation
(b) the third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for anti-Money Laundering and Terrorist Financing purposes
(c) the MLCO has assessed the Client identification and due diligence procedures implemented by the third person and has found them to be in line with the Law and the Directive. A record of the assessment should be prepared and kept in a separate file maintained for each third person
(d) the third person makes available to the Company all the data and documents prescribed in point (1) of Section 10.10 of the Manual.

10.8.6. "Politically Exposed Persons" accounts

The Company shall apply the following with respect to the accounts of "Politically Exposed Persons":

1. The establishment of a Business Relationship or the execution of an Occasional Transaction with politically exposed persons, may expose the Company to enhanced risks, especially if the potential Client seeking to establish a Business Relationship or the execution of an Occasional Transaction is a PEP, a member of his immediate member or a close associate that is known to be associated with a PEP.
   The Company shall pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards.
2. In order to effectively manage such risks, the Company shall assess the countries of origin of its Clients in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the FATF, according to Section 10.8.8 of the Manual.

With regard to the issue of corruption, one useful source of information is the Transparency International Corruption Perceptions Index which can be found on the website of Transparency International at https://www.transparency.org/.

With regard to the issue of adequacy of application of the 40+9 recommendations of the FATF, the Company shall retrieve information from the country assessment reports prepared by the FATF or other regional bodies operating in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) or the International Monetary Fund.

3. The meaning 'Politically Exposed Persons' includes the natural persons to whom or who have been entrusted with the following prominent public functions in the Republic or abroad:

   (a) heads of State, heads of government, ministers and deputy or assistant ministers,
   (b) members of parliaments or of similar legislative bodies,
   (c) members of governing bodies of political parties,
   (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances,
   (e) members of courts of auditors or of the boards of central banks,
   (f) ambassadors, chargıs d'affaires and high-ranking officers in the armed forces,
   (g) members of administrative, management or supervisory bodies of governmental businesses or stated owned enterprises,
   (h) directors, deputy directors and members of the board of directors or persons holding an equivalent position in an international organization,
   (i) mayors.

4. None of the categories set out in point (3) above shall be understood as covering middle ranking or more junior officials.

5. **"Immediate family members"** of a PEP includes the following persons:
   (a) the spouse, or a person to be treated as a spouse of a PEP,
   (b) the children of a PEP, the spouses of the children of a PEP or persons treated as a spouse of children of a PEP,
   (c) the parents of a PEP.

6. **"Persons known to be close associates"** of a PEP means a natural person:
   (a) who is known to be joint beneficial owner of a legal entity or legal arrangement, or is connected to any other close business relationship with a PEP,
   (b) who is the sole beneficial owner of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of a PEP.

7. Without prejudice to the application, on a risk-sensitive basis, of enhanced Client due diligence measures (Section 10.8.1 of the Manual), where a person has ceased to be entrusted with a prominent public function within the meaning of a PEP above for a period of at least one year, the Company shall not be obliged to consider such a person as politically exposed. when a PEP has ceased to exercise prominent public function in the Republic or in a Member State or in a third country or to hold a prominent public position in an international organization, the Company should take into account the risk that that person continues to pose and should take the appropriate measures, depending on the

degree of risk, for a period of at least twelve (12) months, until it is considered that that person no longer poses a risk which specifically characterizes PEPs.

8. Without prejudice to the provisions of point (c) Section 11.8.1 of the Manual, the Company adopts the following additional due diligence measures when it establishes a Business Relationship or carry out an Occasional Transaction with a PEP:

   (a) the Company puts in place appropriate risk management procedures to enable it to determine whether a prospective Client is a PEP. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the Client himself or from publicly available information. In the case of legal entities and arrangements, the procedures will aim at verifying whether the Beneficial Owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute PEPs. In case of identifying one of the above as a PEP, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in this Section of the Manual
   (b) the decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken by an *Executive Director* of the Company and the decision is then forwarded to the MLCO. When establishing a Business Relationship with a Client (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the Business Relationship by an *Executive Director* of the Company which is then forwarded to the MLCO
   (c) before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the Company shall obtain adequate documentation to ascertain not only the identity of the said person but also to assess his business reputation (e.g. reference letters from third parties)
   (d) the Company shall create the economic profile of the Client by obtaining the information specified in Section 10.5. The details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the account. The profile shall be regularly reviewed and updated with new data and information. The Company shall be particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks
   (e) the account shall be subject to annual review in order to determine whether to allow its continuance of operation. A short report shall be prepared summarising the results of the review by the person who is in charge of monitoring the account. The report shall be submitted for consideration and approval to the Board and filed in the Client's personal file.

10.8.7. Electronic gambling/gaming through the internet

The Company shall apply the following with respect to accounts related to electronic gambling/gaming through the internet:

1. The Company may establish a Business Relationship or execute an Occasional Transaction in the names of persons who are involved in the abovementioned activities provided that these persons are licensed by a competent authority of a country of the EEA or a third country which has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the Company. For this purpose, the Company shall request and obtain, apart from the data and information required by the Manual, copy of the licence that has been granted to the said persons by the competent supervisory/regulatory authority, the authenticity of which must be verified either directly with the supervisory/regulatory authority or from other independent and reliable sources.

2. Furthermore, the Company shall collect adequate information so as to understand the Clients' control structure and ensure that the said Clients apply adequate and appropriate systems and procedures for Client identification and due diligence for the prevention of money laundering and terrorist financing.

3. In the case that the Client is a person who offers services (e.g. payment providers, software houses, card acquirers) to the persons mentioned in point (1) above, then the Company shall request and obtain, apart from the data and information required by the Manual, adequate information so as to be satisfied that the services are offered only to licensed persons. Also, it will obtain information necessary to completely understand the ownership structure and the group in which the Client belongs, as well as any other information that is deemed necessary so as to establish the Client's economic profile. Additionally, the Company shall obtain the signed agreement between its Client and the company that is duly licensed for electronic gambling/gaming activities through the internet, by a competent authority of a country mentioned in point (1) above.

4. For all the above cases, the decision for the establishment of a Business Relationship or the execution of an Occasional Transaction is taken by an *Executive Director* of the Company and the decision is then forwarded to the MLCO. Moreover, the account of the said Client is closely monitored and subject to regular review with a view of deciding whether or not to permit the continuance of its operation. Accordingly, a report shall be prepared and submitted for consideration and approval to the Board and filed in the Client's personal file.

10.8.8. Clients from countries which inadequately apply FATF's recommendations, EU non-cooperative tax jurisdictions or High Risk Third Countries

1. The FATF 40+9 Recommendations and the EU Commission constitute the primary internationally recognised standards for the prevention and detection of Money Laundering and Terrorist Financing.

2. The Company shall apply the following with respect to Clients from countries which inadequately apply FATF's recommendations, EU non-cooperative tax jurisdictions or High Risk Third Countries:

   (a) exercise additional monitoring procedures and pay special attention to Business Relationships and transactions with persons, including companies and financial institutions, from countries which do not apply or apply inadequately the aforesaid recommendations
   (b) transactions with persons from the said countries, for which there is no apparent economic or visible lawful purpose, are further examined for the establishment of their economic, business or investment background and purpose. If the Company cannot be fully satisfied as to the legitimacy of a transaction, then a suspicious transaction report is filed to the Unit, according to point (g) Section 6.2 of the Manual.
   (c) with the aim of implementing the above, the Head of the Administration/Back Office Department and the MLCO shall consult the country assessment reports prepared by the FATF (http://www.fatf-gafi.org), the other regional bodies that have been established and work on the principles of FATF [e.g. Moneyval Committee of the Council of Europe (https://www.coe.int/en/web/moneyval/)] and the International Monetary Fund (https://www.imf.org/external/index.htm). Based on the said reports, the MLCO assesses the risk from transactions and Business Relationships with persons from various countries and decides of the countries that inadequately apply the FATF's recommendations. According to the aforesaid decision of the MLCO, the Company applies, when deemed necessary, enhanced due diligence measures for identifying and monitoring transactions of persons originating from countries with significant shortcomings and strategic deficiencies in their legal and administrative systems for the prevention of Money Laundering and Terrorist Financing.

10.9. Client Identification and Due Diligence Procedures (Specific Cases)

The MLCO shall ensure that the appropriate documents and information with respect to the following cases shall be duly obtained, as applicable and appropriate:

10.9.1. Natural persons residing in the Republic

1. The Company shall obtain the following information to ascertain the true identity of the natural persons residing in the Republic:

(a) true name and/or names used as these are stated on the official identity card or passport
(b) full permanent address in the Republic, including postal code
(c) telephone (home and mobile) and fax numbers
(d) e-mail address, if any
(e) date and place of birth
(f) nationality and
(g) details of the profession and other occupations of the Client including the name of employer/business organisation.

2. In order to verify the Client's identity/name the Company shall request the Client to present an original document which is issued by an independent and reliable source that carries the Client's photo (e.g. Passport, National Identity cards, Driving License etc). After the Company is satisfied for the Client's identity from the original identification document presented, it will keep copies.

   It is provided that, the Company shall be able to prove that the said document is issued by an independent and reliable source. In this respect, the MLCO shall be responsible to evaluate the independence and reliability of the source and shall duly document and file the relevant data and information used for the evaluation, as applicable.

3. The Client's permanent address shall be verified using one of the following ways:

   (a) visit at the place of residence (in such a case, the Company employee who carries out the visit prepares a memo which is retained in the Client's file), and
   (b) the production of a recent (up to 6 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid (to protect against forged or counterfeit documents, the prospective Clients are required to produce original documents).

4. In addition to the above, the procedure for the verification of a Client's identity is reinforced if the said Client is introduced by a reliable staff member of the Company, or by another existing reliable Client who is personally known to a member of the Board. Details of such introductions are kept in the Client's file.

5. In addition to the above, the Company shall require and receive information on public positions which the prospective Client holds or held in the last twelve (12) months as well as whether he is a close relative or associate of such individual, in order to verify if the Client is a PEP.

10.9.2. Natural persons not residing in the Republic

1. The Company shall obtain the information described in Section 10.9.1 to ascertain the true identity of the natural persons not residing in the Republic.

2. In addition to the information collected according to Section 10.9.1, without prejudice to the application on a risk-sensitive basis, the Company shall require and receive information on public positions which the prospective Client holds or held in the last twelve (12) months as well as whether he is a close relative or associate of such individual, in order to verify if the Client is a PEP.

3. Furthermore, passports shall always be requested from the Clients not residing in the Republic and, if available, official national identity cards issued by the competent authorities of their country of origin shall be obtained. Certified true copies of the pages containing the relevant information from the said documents shall also be obtained and kept in the Client's files.

   In addition, if in doubt for the genuineness of any document (passport, national identity card or documentary evidence of address), the Company shall seek verification of identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the Client's country of residence.

4. In addition to the aim of preventing Money Laundering and Terrorist Financing, the abovementioned information is also essential for implementing the financial sanctions imposed against various persons by the United Nations and the European Union. In this respect, passport's number, issuing date and country as well as the Client's date of birth always appear on the documents obtained, so that the Company would be in the position to verify precisely whether a Client is included in the relevant list of persons subject to financial sanctions which are issued by the United Nations or the European Union based on a United Nations Security Council's Resolution and Regulation or a Common Position of the European Union's Council respectively.

10.9.3. Joint accounts

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, are verified according to the procedures set in Sections 10.9.1 and 10.9.2 above.

10.9.4. Accounts of unions, societies, clubs, provident funds and charities

In the case of accounts in the name of unions, societies, provident funds and charities, the Company ascertains their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure

rules and registration documents with the competent governmental authorities (in case the law requires such registration).

Furthermore, the Company shall obtain a list of the members of board of directors/management committee of the abovementioned organisations and verifies the identity of all individuals that have been authorised to manage the account according to the procedures set in Sections 10.9.1 and 10.9.2.

10.9.5. Accounts of unincorporated businesses, partnerships and other persons with no legal substance

1. In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, Beneficial Owners and other individuals who are authorised to manage the account shall be verified according to the procedures set in Sections 10.9.1 and 10.9.2.

   In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate shall be obtained.

2. The Company shall obtain documentary evidence of the head office address of the business, ascertains the nature and size of its activities and receives all the information required according to Section 10.5 for the creation of the economic profile of the business.

3. The Company shall request, in cases where exists, the formal partnership agreement and shall also obtain mandate from the partnership authorising the opening of the account and confirming authority to a specific person who will be responsible for its operation.

10.9.6. Accounts of legal persons

1. For Clients that are legal persons, the Company shall establish that the natural person appearing to act on their behalf, is appropriately authorised to do so and his identity is established and verified according to the procedures set in Sections 10.9.1 and 10.9.2.

2. The Company shall take all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as ***the verification of the identity of the natural persons*** who are the Beneficial Owners and exercise control over the legal person according to the procedures set in Sections 10.9.1 and 10.9.2.

3. The verification of the identification of a legal person that requests the establishment of a Business Relationship or the execution of an Occasional Transaction, comprises the ascertainment of the following:

(a) the registered number
(b) the registered corporate name and trading name used
(c) the full addresses of the registered office and the head offices
(d) the telephone numbers, fax numbers and e-mail address
(e) the members of the board of directors
(f) the individuals that are duly authorised to operate the account and to act on behalf of the legal person
(g) the Beneficial Owners of private companies and public companies that are not listed in a Regulated Market of an EEA country or a third country with equivalent disclosure and transparency requirements
(h) the registered shareholders that act as nominees of the Beneficial Owners
(i) the economic profile of the legal person, according to the provisions of Section 10.5.

4. For the verification of the identity of the legal person, the Company shall request and obtain, among others, original or certified true copies of the following documents:

(a) certificate of incorporation and certificate of good standing (where available) of the legal person
(b) certificate of registered office
(c) certificate of directors and secretary
(d) certificate of registered shareholders in the case of private companies and public companies that are not listed in a Regulated Market of an EEA country or a third country with equivalent disclosure and transparency requirements
(e) memorandum and articles of association of the legal person
(f) a resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it
(g) in the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the Beneficial Owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the Beneficial Owner has been agreed
(h) documents and data for the verification, according to the procedures set in Sections 10.9.1 and 10.9.2, of the identity of the persons that are authorised by the legal person to operate the account, as well as the registered shareholders and Beneficial Owners of the legal person.

5. Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a legal person, the Company shall obtain copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

6. For legal persons incorporated outside the Republic, the Company requests and obtains documents similar to the above.

7. As an additional due diligence measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the

Registrar of Companies and Official Receiver of the Republic (for domestic companies) or from a corresponding authority in the company's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as an operating company in the records of the Registrar of Companies and Official Receiver of the Republic or by an appropriate authority outside the Republic.

It is pointed out that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal person, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal person via its account with respect to Money Laundering and Terrorist Financing activities, then it is imperative that further enquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Company for the legal person and all additional documentation and information for updating the economic profile of the legal person is collected.

8. In the case of a Client-legal person that requests the establishment of a Business Relationship or the execution of an Occasional Transaction and whose direct/immediate and principal shareholder is another legal person, registered in the Republic or abroad, the Company, before establishing a Business Relationship or executing an Occasional Transaction, shall verify the ownership structure and the identity of the natural persons who are the Beneficial Owners and/or control the other legal person.

9. Apart from verifying the identity of the Beneficial Owners, the Company shall identify the persons who have the ultimate control over the legal person's business and assets. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal person without requiring authorisation and who would be in a position to override the internal procedures of the legal person, the Company, shall verify the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than 10% in the legal person's ordinary share capital or voting rights.

10. In cases where the Beneficial Owner of a legal person, requesting the establishment of a Business Relationship or the execution of an Occasional Transaction, is a trust set up in the Republic or abroad, the Company shall implement the following procedure:

    (a) the Company shall ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and Beneficial Owners, according to the procedures set in Sections 10.9.1 and 10.9.2
    (b) furthermore, the Company shall ascertain the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other relevant information from the

trustees. All relevant data and information should be recorded and kept in the Client's file.

10.9.7. Investment funds, mutual funds and firms providing financial or investment services

1. The Company shall establish and maintain Business Relationships or execute Occasional Transactions with persons who carry out the above services and activities which are incorporated and/or operating in countries of the EEA or a third country which has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the Company, provided that the said persons:

   (a) possess the necessary license or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services, and
   (b) are subject to supervision for the prevention of Money Laundering and Terrorist Financing purposes.

2. In the case of the establishment of a Business Relationship or the execution of an Occasional Transaction with persons who carry out the above services and activities and which are incorporated and/or operating in a third country other than those mentioned in point (1) above, the Company shall request and obtain, in addition to the abovementioned, in previous points, documentation and the information required by the Manual for the identification and verification of persons, including the Beneficial Owners, the following:

   (a) a copy of the license or authorisation granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other independent and reliable sources, and
   (b) adequate documentation and sufficient information in order to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the Client.

3. In the case of investment funds and mutual funds the Company, apart from identifying Beneficial Owners, shall obtain information regarding their objectives and control structure, including documentation and information for the verification of the identity of investment managers, investment advisors, administrators and custodians.

10.9.8. Nominees or agents of third persons

1. The Company shall take reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity, according to the procedures set in Sections 10.9.1 and 10.9.2 of the Manual:

   (a) the nominee or the agent of the third person, and
   (b) any third person on whose behalf the nominee or the agent is acting.

2. In addition, the Company shall obtain a copy of the authorisation agreement that has been concluded between the interested parties.

10.10. Reliance on Third Persons for Client Identification and Due Diligence Purposes

1. The Company may rely on third persons for the group implementation of points (a), (b) and (c) of Client identification and due diligence procedures, provided that:

   (a) The third person ***makes immediately available*** to the Company all evidence, data, information and identification documents which must be certified true copies of the originals or as otherwise acceptable by current CySEC practices, that were collected during the process of identification and Client due diligence, and forward directly to the Company copies of the documents and information on the identity of the Client and the beneficial owner. Client
   (b) The Company applies the appropriate due diligence measures on the third person with respect to his professional registration and procedures and measures applied from the third person for the prevention of Money Laundering and Terrorist Financing, according to the provisions of the Directive.
   (c) **The ultimate responsibility for meeting those requirements of Client identification and due diligence shall remain with the Company who relies on the third person**.

2. For the purposes of this Section of the Manual, third person means credit institutions or financial institutions or auditors or accountants or tax advisors or consultants or independent legal professionals or person providing to third party trust and company services included in the definition of the term "Financial Activities" above, falling under the EU Directive and which are active in the Republic or in another country of the EEA which:

   (a) they are subject to mandatory professional registration, recognised by law,
   (b) they apply customer due diligence measures, reply on record-keeping and programmes against ML and TF in accordance with the EU Directive or equivalent regulations, and
   (c) they are subject to supervision regarding their compliance with the requirements of the EU Directive.

3. Further to point 2 above, third person for the purposes of this Section of the Manual may also be any other person who is engaged in financial business (as defined in Section 2 of the Law), or auditors or accountants or tax advisors or consultants or independent legal professionals or persons providing to third parties trust and company services as included in the definition of the term "Financial Activities" and who operate in countries outside the EEA and which has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the Company.

   It is provided that the abovementioned third persons have to fulfil the requirements set out in points 2(a) and 2(b) above.

4. For the purposes of this Section of the Manual, 'third parties' means **obliged entities** listed under the definition of "Financial Activities" above, the member organisations or federations of those obliged entities, or other institutions or persons situated in a Member State or third country that:

   a. apply Client due diligence requirements and record-keeping requirements that are consistent with those laid down in the Directive, and
   b. have their compliance with the requirements of the Directive supervised in a manner consistent with the Directive.

5. The Company is prohibited from relying on third parties established in High Risk Third Countries.

6. It should be ensured that the Company shall obtain from the third party relied upon the necessary information concerning the Client due diligence requirements.

7. It should be ensured that the Company to which the Client is referred take adequate steps to ensure that the third party provides, immediately, upon request, relevant copies of identification and verification data and other relevant documentation on the identity of the Client or the beneficial owner.

8. The Company shall ensure that the policies and procedures referred to in the above paragraph are effectively applied at the level of branches and subsidiaries majority-owned in Member States and third countries as and if applicable
   It should be noted that the out outsourcing of tasks related to AML/CFT to service providers established in third countries should be subject to additional safeguard measures in order to ensure that the outsourcing does not, as a result of the location of the service provider, increase the risk of non-compliance with the legal and regulatory requirements or of inefficient performance of the outsourced tasks, nor hinders the

competent authority's capacity to effectively exercise its supervisory power with regard to the service provider.

The Company shall ensure that the third person gives its written approval for such cooperation which should be kept in the third person's personal file.
The Company shall keep a record with the information of the third party to which it relies for Client Identification and Due Diligence Purposes.

9. In the case of a group, the Company will be considered to apply sufficient measures through the programme of its group as along as all following conditions are met:

   (a) The Company relies on information provided by a third party which belongs to the same group;
   (b) The said group applies Client due diligence measures, rules on record keeping and programmes against money laundering and terrorist financing in accordance with the requirements of the EU Directive or equivalent rules;
   (c) The effective implementation of the requirements referred to in paragraph (b) is supervised at group level by the competent supervisory authority of the home member state or of the third country.

10. In relation to the electronic identity verification, third parties should also satisfy the conditions in paragraph 2 of Section 10.8.2 of this Manual.

11. The Company may rely on third persons only at the outset of establishing a Business Relationship or the execution of an Occasional Transaction for the purpose of verifying the identity of their Clients. According to the degree of risk any additional data and information for the purpose of updating the Client's economic profile or for the purpose of examining unusual transactions executed through the account, is obtained from the natural persons (directors, Beneficial Owners) who control and manage the activities of the Client and have the ultimate responsibility of decision making as regards to the management of funds and assets.

12. Further to point 3 above, in the case where the third person of subparagraph (1) is an auditor or accountant or tax advisor or consultant or an independent legal professional or a trust and company services provider from a country which is a member of the EEA or a third country which has not been identified by the EU Commission as high-risk third country, as well as in other cases of higher risk identified by Member States or the Company itself, then the Company, before accepting the Client identification data verified by the said third person, shall apply the following additional measures/procedures:

   (a) the MLCO or the appointed person shall assess and evaluate, according to point (l) of Section 6.2 of this Manual, the systems and procedures applied by the third person for the prevention of Money Laundering and Terrorist Financing, as applicable

(b) as a result of the assessment of point (a) above, the MLCO must be satisfied that the third person implements Client identification and due diligence systems and procedures which are in line with the requirements of the Law and the Directive

(c) the MLCO shall maintain a separate file for every third person of the present paragraph, where it stores the assessment report of point (a) and other relevant information (for example identification details, records of meetings, evidence of the data and information of point 2 above)

(d) the commencement of the cooperation with the third person and the acceptance of Client identification data verified by the third person is subject to approval by the MLCO, according to point (l) of Section 6.2 of the Manual.

13. The Company must request from the third party to:

(a) make immediately available data, information and documents obtained as a result of the application of the procedures establishing identity and Clients due diligence measures in accordance with of points (a), (b) and (c) of Client identification procedures and due diligence measures of Section 10.11 of the Manual,

(b) forward immediately to them, copies of these documents and relevant information on the identity of Client or the beneficial owner which the third party collected when applying the above procedures and measures.

14. Without prejudice to point 3, above, the identification data and information obtained for the Client and beneficial owner, are forwarded immediately from the following third parties to the Company following its request, taking into consideration the degree of risk that arises from the type of the Client, the business relationship, the product or transaction:

(a) Credit institutions or financial organisations that fall under the scope of the EU directive and are active in the Republic or in another country of the EEA

(b) Any third party conducting financial activities (as per the definition) operating outside the EEA which has been determined that it applies requirements equivalent to those laid down in the European Union Directive

It is provided that the abovementioned third persons have to fulfil the requirements set out in points 2(a) and 2(b) above.

15. In the case the Company relies to a third party, applies the following additional measures/procedures:
(a) before the establishment of the business relationship or the carrying out of the occasional transaction applies due diligence measures to the third party;
(b)sign an agreement with the third party specifying the obligations of each party;
(c) maintains a separate file for every third party of the present paragraph, where it stores the relevant information

(d) the commencement of the cooperation with the third party and the acceptance of customer identification data verified by the third party is subject to approval by the compliance officer. (e) The Company shall have access to all available data and information of a customer collected, assessed ad verified by such a third party, at all times.

The Compliance Officer should verify that the third party with whom the Company intends to rely on for the application of the customer identification and due diligence measures and gives his/her written approval for the said reliance, which should be kept in the personal file of the third party.

*NOTE: For the purposes of this Section of the Manual, the terms financial institutions and persons engaged in financial business activities do not include currency exchange offices and money transmission or remittance offices.

**NOTE: For the purposes of this Section of the Manual, the provisions specified herein, do not apply to outsourcing or agency relationships, where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the Company.

The MLCO shall be responsible for the implementation of the provisions mentioned in this Section of the Manual.

The Internal Auditor shall be responsible to review the adequate implementation of the provisions mentioned herein, at least annually.

10.11. Ways of application of Client Identification and Due Diligence Procedures

Client identification procedures and Client due diligence measures shall comprise:

(a) identifying the Client and verifying the Client's identity on the basis of documents, data or information obtained from a reliable and independent source
(b) 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
(c) assessing, and as appropriate, obtaining information on the purpose and intended nature of the business relationship
(d) 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.

(e) Screening Clients against databases or third party checks for adverse tax-related news.

10.12. Client Identification and Due Diligence Procedures at group level

Where the Company is part of a group it shall implement group-wide policies and procedures, including data protection policies and policies, as well as policies and procedures for sharing information within the group (whether in Member State or third country), for the purpose of prevention of money laundering or terrorist financing.

Those policies and procedures shall be implemented effectively at the level of the Obliged entity's branches and majority-owned subsidiaries in Member states and third countries.

Where the Company has establishment in a Member State (i.e. operating facilities) it shall comply with the provisions and national laws of the said Member State. Where the Company has an establishment in a third country (i.e. branch or majority-owned subsidiary) where less strict requirements are applied from those provided in the Law, Directives, and Circulars issued by CySEC for the prevention of money laundering and terrorist financing, the Company shall apply those issued by CySEC to the extent permitted by the laws of the third country.

In the case where the laws of the third country do not permit the application of the policies and procedures mentioned above, the Company is obliged to:

- take additional measures so as to effectively deal with the risk of money laundering or terrorist financing, and;
- inform CySEC immediately.

Nevertheless, it should be noted that the Company Is not authorised to for the ancillary service of *Safekeeping and administration of financial instruments, including custodianship and related services*, therefore it cannot accept any deposits. The Client should fund his trading account with the Brokers he is connected with in order to be bale to use his account with the Company.

10.14. Beneficiaries Information

The Company, acquires and keeps adequate, accurate and up-to-date information on beneficiaries, including the details of them rights held by the beneficial owners.

Moreover, and referred to in paragraph above the company shall ensure the provision of information by the Company on the beneficial owner in a corresponded relationship and in addition, information where due diligence measure have been undertaken. The following persons shall, have access to information on the beneficial owner:

(a) the competent Supervisory Authority, the Unit, the Customs Department, the Tax Department and the Police without any restriction
(b) the Company, in the course of the due diligence and Client identification measures specified in this Law.

Provided that the Company is not solely relying on the information held in the central register of beneficial owners and other legal entities referred to in sub-paragraph (4) in Section 61A of the Law, in order to meet the requirements of the due diligence and Client identification measures. The requirements are met using a risk-based approach.

The Company by the Legitimate Interest shall have access to

- the name,
- month and year of birth,
- nationality and country of residence of the beneficial owner,
- as well as the nature and extent of the rights it holds

Provided that Legitimate Interest means solely the interest of the company in the fight against money laundering and terrorist financing as provided by the Law and the access to information about the beneficial owner is made in accordance with the provisions of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018).

10.15. Cooperation between the competent authorities of the Republic of Cyprus and the competent authorities of the Member States

During the cooperation between the Supervisory Authorities, the Unit, the Police and the Customs Department and respective competent authorities of the Member States of the European Union for the purposes of this Law, the exchange of information or assistance between them is not prohibited and no unreasonable or excessive restrictive conditions are set. in the exchange of information or assistance between them.

Without prejudice to the generality of the provisions of the previous paragraph, the competent authorities of the Republic of Cyprus shall not reject a request from a competent authority of a Member State for assistance on the grounds that (i) the request is deemed to involve tax matters; (ii) national law requires the obligated entity to maintain confidentiality or confidentiality, except in cases where the information requested is protected by legal privilege or professional secrecy, as described in the provisions of paragraphs (f) of Section 69 and Section 44 of the Law (iii) an investigation, inquiry or proceeding is in progress in the requested Member State, unless assistance would prevent such inquiry, inquiry or proceeding and (iv) the nature or situation of the applicant bond competent authority is different from that of the competent authority to which the request is addressed.

10.16. Business relationship with persons who have acquired the Cypriot citizenship under the Cyprus Investment Program

In accordance with Circular C416, the Company shall apply on, a risk-based approach and on an ongoing basis, checks/reviews to identify weather Clients and/or Clients' beneficial owners have acquired, either themselves or their spouses and/or their children, Cypriot citizenship under the Cyprus Investment Program (hereinafter "CIP").

Such checks are performed to, at least, Clients/ Ultimate Beneficial Owners:

- that declared being Cypriot nationals and who provided proof of identity documents issued by the Cypriot authorities (passport/ID), and
- whose economic profile suggests that they have the resources to qualify for a Cypriot citizenship under CIP, e.g., whose net worth (as per their economic profile) exceeds a certain threshold (e.g. net worth over EUR6.0 million or annual income exceeding EUR500.000 or other)
- that declared having more than one nationality (e.g., to the extent possible check for multiple nationalities; where a person has more than one nationality the Company collects and checks each passport separately so as to identify if these include the Cypriot nationality).

Clients and/or Clients' beneficial owners that have acquired, either themselves or their spouses and/or their children, Cypriot citizenship under the Cyprus Investment Program (hereinafter "CIP") shall be categorised as high risk with respect to money laundering and terrorist financing risk.

Following the attainment of the citizenship and in the event that the firm continues to maintain a business relationship with the client (through the provision of other services that fall within the scope of the Law), the firm should consider this in its continuous risk assessment process for the particular client.

10.17. National Risk Assessment of Money Laundering and Terrorist Financing Risks (NRA)

The first National Risk Assessment of Money Laundering and Terrorist Financing Risks (NRA) for Cyprus was published on the website of the Ministry of Finance on 30 November 2018. The NRA falls within the actions undertaken by the Cypriot authorities in order to identify, assess and understand the country's money laundering and terrorist financing threats and vulnerabilities. This was also in compliance with the relevant Recommendations of the Financial Action Task Force, as well as the provisions of the 4th EU AML/CFT Directive, which have been transposed into domestic legislation. In particular, the NRA provides appropriate information to the regulated entities in order to carry out their own risk assessment of money laundering and terrorist financing

The Company shall examine the NRA as its content should be taken into account when assessing money laundering and terrorist financing risks, thereby improving the effectiveness of the measures and procedures applied. Based on the NRA results, an action plan which includes measures/actions to remedy the vulnerabilities identified and recorded in the NRA has been prepared.

10.18. Ultimate Beneficial Owners (hereinafter "UBOs") Central Registry

The UBO Register shall be published by the Registrar of Companies and Official Receiver (hereinafter "RoC"), who has been appointed as the competent authority for maintaining the UBO Register. The RoC shall keep information about the companies and other legal entities and their beneficial owners.

The competent Supervisory Authority, the AML Unit, the Customs Department, the Tax Department and the Police shall have access to the information about a beneficial owner through the UBO Register if they have a legitimate interest and, upon submission of a formal request at the RoC. The Company shall have access in the context of undertaking due diligence and identification measures for its Clients. All members of the general public will have only limited access, which consists of access to the name, month and year of birth, citizenship and country of residence of the beneficial owner, as well as the type and extent of rights that the shareholders hold in the Company.

It should be noted that all beneficial owners through shares, voting rights, ownership interest, bearer shareholdings control via other means shall provide to the corporate and other legal entities all the necessary information.

The verification of the identity of the Client and the beneficial owner shall take place before the establishment of a business relationship or the carrying out of the transaction. The Company must collect proof of registration in the registry as part of its due diligence procedures.

11. ON-GOING MONITORING PROCESS

11.1. 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 Unit, according to point (g) of Section 6.2 and Section 13 of the Manual.

The constant monitoring of the Clients' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing.

In this respect, the MLCO shall be responsible for maintaining as well as developing the on-going monitoring process of the Company. The Internal Auditor shall review the Company's procedures with respect to the on-going monitoring process, at least annually.

The MLCO implements a Risk based approach for the on-going monitoring procedures of the Company, which is based on, inter alia, the Clients' categorisation and the volume of transactions estimated in the pre-account information provided. Relevant employees perform reviews of Clients' transactions at least once a week, or otherwise if requested by the MLCO, and reports to the MLCO their finding for the purposes of the on-going monitoring of the

Company. The responsible employee shall also provide daily records of Clients' incoming and outgoing money transfers, to the MLCO.

The MLCO monitors and ensures, on a frequent basis, that the actual amount of funds deposited by Clients is consistent with the amount of funds indicated during the Client account opening stage, as well as with the economic profile of the Client.

Additionally, all employees must be alert to detect and report internally any activity on the Client's account or behaviour, which is inconsistent with the previously disclosed/obtained information. Employees must inform accordingly the MLCO, (See also Section 11.2 below)

11.2. Procedures

The procedures and intensity of monitoring Clients' accounts and examining transactions on the Client's level of risk shall include the following:

(a) 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 head of the department providing the relevant investment and/or ancillary service or any other person who identified the unusual or suspicious transactions as well as the Head of the Administration/BackOffice Department shall be responsible to communicate with the MLCO

(b) further to point (a) 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

(c) the ascertainment of the source and origin of the funds credited to accounts

(d) the on-going monitoring of the business relationship in order to determine[1] whether there are reasonable grounds to suspect that Client accounts contain proceeds derived from serious tax offences.

(e) the use of appropriate and proportionate IT systems, including:
- adequate automated electronic management information systems which will be capable of supplying the Board of Directors 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

[1] Albeit the Company is not expected to determine if clients are fully compliant with all their tax obligations globally.

money laundering or terrorist financing 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.

(f) the monitoring of accounts and transactions shall be carried out 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

(g) the monitoring of accounts held by Clients' whose identity was verified via the use of video communication, in accordance to Section 10.8.2 of this Manual.

(h) the monitoring on ongoing basis of the transactions of *low risk* Clients to ensure that there are no suspicious transactions.

11.3. Validity of KYC documentation

The Company should have in place adequate procedures and/or systems via which the validity of the KYC documentation provided (i.e., ID, passport) is monitored in respect to their validity period, which should include alerts and/or notifications for the upcoming expiration.

Two (2) months prior the expiration of the KYC documentation, the Administration/Back Office Department is responsible to inform the Client and request a renewed valid KYC documentation. A reminded should be send one (1) month prior the expiration date. Records of the aforementioned notifications and reminders should be kept in the Company's records.

11.4. On-going update of KYC and Due Diligence documentation

11.4.1. Full review and update

Depending on their risk categorisation, a review of the KYC and Due Diligence should be conducted, during which recent information and/or valid documentation should be requested by the Client, in the frequency as specified below:

a. Low Risk Clients: every three (3) years

b. Normal Risk Clients: every two (2) year
c. High Risks Clients: Yearly

11.4.2. Soft review

The Administration/Back Office Department is responsible to request via email/notification from Clients categorised as Low or Normal Risk (as per Sections 9.2.1 and 9.2.2) on an annual basis to either confirm that the KYC and Diligence information and/or documentation kept in the Company's records remains the same or has changed/updated. In case the Client confirm that any change and/or update has taken place, then a Full review as per Section 11.4.1 should be conducted.

11.4.3. Failure or Refusal to Submit Information for the Update of Clients Profile

Failure or refusal by the Client to submit timely updated and/or valid information and/or documentation requested as per Sections 11.4.1 and 11.4.2 should conclude to the termination of the Client Relationship by the Company.

12. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS / ACTIVITIES TO THE UNIT

12.1. Registration for submission of Suspicious Transactions/Activities to the Unit

The Company is required to register with the goAML IT System in order for the submission of suspicious transactions/activities to the Unit to be performed in accordance to the provisions of CySEC's Circular C058 and the Directive issued by the Unit relating to the amended procedures followed for the submission of suspicious transactions/activities to the Unit.

12.2. Reporting of Suspicious Transactions to the Unit

The Company, in cases where there is an attempt of executing transactions or of transactions being executed, irrespective of the amount and which knows or has reasonable grounds to suspect that are related to money laundering or terrorist financing, reports, through the MLCO its suspicion to the Unit shall be in accordance with point (g) of Section 6.2 and Section 12 of the Manual.

The Company, its directors and employees are not allowed to disclose to the Client or third parties the fact that information on suspicious transactions has been transmitted, is being transmitted or will be transmitted to the Unit or that there is or that an analysis of such information or suspicious transactions can be carried out in relation to money laundering or terrorist financing.

No person is allowed to make any disclosure that may interfere with, or adversely affect, inquiries and inquiries conducted on the calibration of revenue or the commission of specified offenses, knowing or suspecting that the above investigations are being conducted and surveys.

12.3. Suspicious Transactions

1. The definition of a suspicious transaction as well as the types of suspicious transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. A suspicious transaction will often be one which is inconsistent with a Client's known, legitimate business or personal activities or with the normal business of the specific account, or in general with the economic profile that the Company has created for the Client. The Company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

2. Examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing are listed in Appendix 3 of the Manual. The relevant list is not exhaustive nor it includes all types of transactions that may be used, nevertheless it can assist the Company and its employees (especially the MLCO and the Head of the Administration/Back Office Department) in recognising the main methods used for Money Laundering and Terrorist Financing. The detection by the Company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

3. In order to identify suspicious transactions the MLCO shall perform the following activities:
   - monitor on a continuous basis any changes in the Client's financial status, business activities, type of transactions etc
   - monitor on a continuous basis if any Client is engaged in any of the practices described in the list containing examples of what might constitute suspicious transactions/activities related to Money Laundering and Terrorist Financing which is mentioned in Appendix 3 of this Manual.

   Furthermore, the MLCO shall perform the following activities:

   - receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report. The said reports are archived by the MLCO

- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLCO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file
- if, as a result of the evaluation described above, the MLCO decides to disclose this information to the Unit, then he prepares a written report, which he submits to the Unit, according to point (g) of Section 6.2 and Section 12.4 below
- if as a result of the evaluation described above, the MLCO decides not to disclose the relevant information to the Unit, then he fully explain the reasons for his decision on the Internal Evaluation Report.

12.4. MLCO's Report to the Unit

According to Circular C058, all the reports of the MLCO of point (g) of Section 6.2 of the Manual shall be submitted to the Unit through the **goAML Professional Edition (PE)**", by the completion of the online report on the web-application of the UNIT or by the completion of the relevant XML Report.

After the submission of a suspicious report of point (g) of Section 6.2 of the Manual, the Company may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Company exercises particular caution, according to Section 48 of the Law, not to alert the Client concerned that a suspicious report has been submitted to the Unit. Close liaison with the Unit is, therefore, maintained in an effort to avoid any frustration to the investigations conducted.

After submitting the suspicious report of point (g) of Section 6.2 of the Manual, the Company adheres to any instructions given by the Unit and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

According to Section 26(2)(c) of the Law, the Unit may instruct the Company to refrain from executing or delay the execution of a Client's transaction without such action constituting a violation of any contractual or other obligation of the Company and its employees.

Furthermore, after the submission of a suspicious report of point (g) of Section 6.2 of the Manual, the Clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the MLCO.

12.5. Submission of Information to the Unit

The Company shall ensure (see also Section 12 of the Manual) that in the case of a suspicious transaction investigation by the Unit, the MLCO will be able to provide without delay the following information:

(a) the identity of the account holders
(b) the identity of the Beneficial Owners of the account
(c) the identity of the persons authorised to manage the account
(d) data of the volume of funds or level of transactions flowing through the account
(e) connected accounts
(f) in relation to specific transactions:
- the origin of the funds
- the type and amount of the currency involved in the transaction
- the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers
- the identity of the person that gave the order for the transaction
- the destination of the funds
- the form of instructions and authorisation that have been given
- the type and identifying number of any account involved in the transaction.

12.6. Protection of Persons Reporting

Bona fide disclosure of information by the Company or by an employee or director of the Company does not constitute a breach of any contractual or statutory, regulatory or administrative prohibition of disclosure of information, nor implies any liability for the Company or its directors or employees, even if the circumstances did not allow them to know precisely what the main illegal activity was and regardless of whether it was actually committed Illegal activity.

Persons who submit an internal report or report to the Unit for suspicious transactions shall be protected against any threat or hostile action and in particular by adverse acts or discrimination in the workplace.

Persons exposed to threats, retaliation or hostile actions, and in particular adverse actions or discrimination in the workplace on the grounds of having submitted internal reports or reports to the Unit for suspicious transactions under the provisions of Section 69 of the Law, have the right to submit a complaint to CySEC.

12.7. Disclosure in Good Faith

Disclosure of information in good faith by the Company or by an employee or director of the Company, in accordance with the provisions of section 69 of the Law, shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the Company or its directors or employees in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred.

12.8. Prohibition from Carrying out Suspicious Transactions Before Informing the Unit

The Company shall refrain from carrying out transactions which it knows or suspects to be related with money laundering or terrorist financing, before it informs the Unit of its suspicion in accordance with sections 27 and 69 of the Law. In case it is impossible to refrain from carrying out the transaction or is likely to frustrate efforts to pursue the persons of a suspected money laundering or terrorist financing operation, the Company, must inform the Unit immediately afterwards.

12.9. Prohibition of the Collection of cash for the sale of Goods

It is prohibited for a person trading in precious stones and/or precious metal s, mechanical vehicles, works of art and/or antiques, within the framework of its business activities to receive any amount equal to or higher than EUR 10.000 in cash, irrespective of whether the transaction is carried out in a single operation or in several operations which appear to be linked.

The non-application of this prohibition is considered to be a criminal offence and is subject to penalty of not more than ten percent (10%) of the amount received in cash.

12.10. Exemption from the prohibition of information disclosure

Disclosure of information shall not be prohibited, in accordance with the provisions of Section 49 of the Law, between:

(a) credit institutions and financial institutions, or between the above institutions and their branches and majority-owned subsidiaries located in third countries, provided that those branches and majority-owned subsidiaries fully comply with the group-wide policies and procedures, including procedures for sharing information within the group.
(b) persons performing professional activities of auditors, external accountants, tax advisors and independent legal professionals, who perform their professional activities, whether as employees or not, within the same legal person or a larger structure to which the legal person belongs, and which shares common ownership, management or compliance control.
(c) relevant obliged entities that have the same Client and that they are from the same professional category and are subject to obligations as regards professional secrecy and personal data protection.

Disclosure and exchange of information performed in accordance with points a, b and c above, shall not be considered as a breach of any contractual or other legal obligation on information disclosure.

13. UNITED NATIONS (UN) AND EUROPEAN UNION (EU) SANCTION REGIMES

The Law that provides for the Implementation of the Provisions of the United Nations Security Council Resolutions or Decisions (Sanctions) and the European Union Council's Decisions and Regulations (Restrictive Measures) is Law 58(I)/2016. In accordance with the said Law, CySEC is responsible for the compliance of the regulated entities with the Sanctions/Restrictive Measures that are decided and imposed by the United Nations' Security Council and the European Union.

International sanctions are political and economic decisions that are part of diplomatic efforts by countries, multilateral or regional organizations against states or organizations either to protect national security interests, or to protect international law, and defend against threats to international peace and security. These decisions principally include the temporary imposition on a target of economic, trade, diplomatic, cultural or other restrictions (sanctions measures) that are lifted when the motivating security concerns no longer apply, or when no new threats have arisen.

Furthermore, the Combating of Terrorism and Victims' Protection Law (L.75(I)/2019) deals with a number of issues, including the definition of terrorism felonies, the responsibilities of legal persons, responsibility of entities obliged under the AML/CFT Law to confiscate property belonging or controlled by persons engaged in terrorism and the responsibility of supervisory authorities for ensuring that obliged entities abide with the relevant provisions of this law. The Ministry of Foreign Affairs website (Theme 'Sanctions') lists relevant information regarding Sanctions/Restrictive Measures.

Further to the above, and for timely, valid and immediate updates on current European Union (EU) restrictive measures and United Nations (UN) sanctions, the Company consults the following links to this respect:

For EU restrictive measures:

- EU Sanctions Map
- Consolidated List of Sanctions
- European Union External Action Service
- European Commission
- Council of the European Union
- Official Journal of the European Union
- Common Foreign and Security Policy (CFSP)

For UN sanctions:

- General Information
- Consolidated List of Sanctions
- United Nations Security Council Resolutions

- United Nations Office on Drugs and Crime

The Company drafts and enforces measures and procedures for the identification of activities and/or transactions which breach or may potentially breach the provisions of the Resolutions or Decisions of the Security Council ("Sanctions") and/or Decisions and Regulations of the Council of the European Union ("Restrictive Measures"), as defined by Sanctions Law (The Implementation of Provisions of Resolutions of Decisions of the United Nations Security Council (Sanctions) and the Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law of 2016 (Law 58(I)/2016)).

In the event that the Company intends to take action which falls within the cases that may be approved under the Sanctions and/or Restrictive Measures, submits, through the Company's MLCO, prior to the transaction, a request to the Member of the Unit for the Implementation of Sanctions or the relevant Credit Institution for submission to the Advisory Committee on Economic Sanctions, depending on the circumstances, for approval or rejections.

The Company shall record the measures and procedures for the identification of acts that violate or potentially violate the provisions of the Sanctions or Restrictive Measures.

The Company shall perform screening of its Clients against applicable financial sanctions target lists published in Cyprus Ministry of Exterior Consolidated Lists (http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument).

The Company shall create a Sanctions Compliance Program (SCP) which it will include controls, policies, and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to activity that may be prohibited by the regulations and laws administered relating to Sanctions. The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to sanctions compliance (including reporting and escalation chains), and minimize the risks identified by the organization's risk assessments.

An effective training program shall be an integral component of a successful SCP. The training program should be provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments.

Senior Management should ensure that the SCP receives adequate resources and is fully integrated into the organization's daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.

The Company shall monitor on an ongoing basis its Clients and Clients' related entities, directors and beneficial owners. The Company shall prepare and continually update a list of countries which are subject to wider embargoes and ensuring that services are not supplied to persons and legal entities in those countries, either directly or through indirectly (through an intermediary).

In addition, the Company shall follow the procedure below in relation to Sanction List(s):

a. to study the notifications in Section "Sanctions/Restrictive Measures" on CySEC's website and assess whether the Sanctions/Restrictive Measures contained therein affect its customers.
b. to consider the OFAC'S Specially Designated Nationals List (SDN List) which is updated regularly, when assessing the money laundering (ML) and terrorist financing (TF) risks associated with business relationships and occasional transactions with its clients
c. to assess or reassess money laundering and terrorist financing risks, in the case of a business relationship with any person subject to Sanctions/Restrictive Measures.
d. in the case of a new/prospective customer who is subject to Sanctions/Restrictive Measures, to avoid the commencement of any business relationship with such a customer.
e. In the case of an existing customer who is subject to Sanctions/Restrictive Measures, to carefully examine the actions/measures that must be implemented (e.g. whether the freezing of funds/accounts is necessary, etc.) in accordance with the relevant UN Security Council Resolutions/Decisions and/or the EU Council's Decisions and Regulations.

In case the World Compliance results show that the prospective Client is included in Sanction Lists, the MLCO notifies the Executive Directors of the Company in order to obtain legal advice, if needed. In complicated or controversial cases and/or when it is deemed necessary, external legal advice and/or opinion should be sought. If the legal advice is not to proceed with the client, the Executive Directors notify the MLCO who notify the client accordingly.

As per the provisions of the Combating of Terrorism Law of 2019 (L.75(I)/2019) any person that provides support, in any way, of persons, groups or entities involved in terrorism as identified from the Resolutions or Decisions of the United Nations Security Council (Sanctions) and the Decisions and Regulations of the Council of the European Union (Restrictive Measures), in case of conviction is subject, to imprisonment not exceeding 8 years or a pecuniary penalty not exceeding €150,000 or both penalties.

14. RECORD-KEEPING PROCEDURES

14.1. General

The Administration/Back Office Department of the Company shall maintain records of:

(a) Copies of documents and information which are necessary to comply with the Client due diligence requirements as defined in the Law and in this Manual including information obtained by means of electronic identification or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by a competent authority of the Republic,
(b) The supporting evidence and records of transactions, consisting of the original documents or copies which are necessary to identify transactions,

(c) The relevant correspondence documents with the Clients and other persons with whom a business relationship is maintained.

The abovementioned documents/data/information shall be kept for a period of five (5) years after the end of the business relationship with the Client or after the date of an occasional transaction.

The Company shall ensure that the above documents may be retained for five (5) additional years in the event that it is reasonably justified to further maintain the documents and information for the purpose of preventing, detecting or investigating money laundering and terrorist financing, without affecting criminal procedure provisions concerning evidence in connection with ongoing criminal investigations and proceedings.

It is provided that the documents/data mentioned in points (a) and (c) above which may be relevant to ongoing investigations shall be kept by the Company until the Unit confirms that the investigation has been completed and the case has been closed.

14.2. Format of Records

The Administration/Back Office Department shall retain the documents/data mentioned in Section 14.3 of the Manual, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Administration/Back Office Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to CySEC or to the Unit, after a relevant request.

In case the Company will establish a documents/data retention policy, the MLCO shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive.

The Internal Auditor shall review the adherence of the Company to the above, at least annually.

14.3. Certification and language of documents

1. The documents/data obtained, shall be in one of the following forms:
   a. original form or
   b. certified true copy form where certification is performed by the Company, in cases where the Company identifies the identity of the Client itself, after presented to the same in its original form, or
   c. certified true copy form where certification is performed by third parties, in cases where they verify the identity of the Client in accordance with the provisions of Section 10.10

d. certified true copy form where the certification is performed by a competent authority or a person who, according to the relevant provisions of the laws of their country, are responsible for the authentication of documents or data. In that case the documents should be certified copies (apostilled or notarised), or
e. provided that at least one of the procedures referred to Section 10.8.2 (2) of this Manual is followed:
    - copy of the original or,
    - data and information collected by electronic means electronic verification.

Authentication by electronic means:

a. Authentication by electronic means is performed either directly by the Entity, or through a third party. The Company and the third parties shall meet the following conditions:
    (i) the electronic databases maintained by the third party or to which the third person or the Company have access or are registered with and approved by the Commissioner Protection of Personal Data for the purpose of safekeeping personal data (or the appropriate competent authority in the country of that database)
    (ii) electronic databases provide access to information that refers to both current and previous situations that indicate that the person actually exists and include positive information (at least full name, address and date of birth of the Client) as well as negative information (eg committing offenses such as identity theft, inclusion in files of deceased persons, inclusion in lists of sanctions and restrictive measures by the Council of the European Union and the Security Council (UN)
    (iii) electronic databases contain a wide range of sources, with information from various time intervals, updated to real-time update and send notifications trigger alerts when important data is differentiated.
    (iv) has established transparent procedures that allow to the Company to identify what information has been searched for, which ones are their effects and their importance in relation to the degree certainty as to the identity of the Client
    (v) have established procedures that allow to the Entity to record and store the information used and the result in relation to identity testing.

b. The information comes from two or more sources. At a minimum, the control procedure by electronic means can fulfils the following indicative matching standard:
    (i) Locate full name and current address Client from a source, and
    (ii) Locate the full Client name and either the current one address or date of birth from a second source.

For purposes of performing identity authentication by electronic means, the Company must establish procedures to ensure that the integrity, validity and reliability of the information it has access to. Provided that the audit process should include both positive and negative information.

Provided that the Company assesses the results of the audit identity to meet the requirements of Section 61(3) of the Code Law. The Obligated Entity establishes

mechanisms for execution quality controls to evaluate the quality of information on which it intends to rely.

2. A true translation shall be attached in the case that the documents of point (1) above are in a language other than Greek of English.

Each time the Company shall proceed with the acceptance of a new Client, the Head Administration/Back Office Department shall be responsible for ensuring compliance with the provisions of points 1 and 2 above.

3. Use of Innovative methods:
   a. The use of an innovative method or a combination of them for the non-face-to-face identification and verification of the identity of natural persons. Such methods may include without limitation identity verification by taking a dynamic real time selfie, and/or of a real time video call. The following conditions shall be meet be cumulatively fulfilled:

      (i) The use of such methods take place on a risk-based approach depending on the level of assets to be deposited and the size of transactions involved.
      (ii) A detailed assessment of the risks emanating from the use of such methods and of the measures employed to mitigate such risks has taken place in advance in accordance with of Part IV of the Directive, whereas such assessment is updated on an ongoing basis and it allows on a reasonable, consistent and demonstrable basis to conclude that the money laundering risks, including the risks of identity theft, impersonation and identity fraud, are sufficiently reduced.
      (iii) Before the Company make use of such innovative methods, it shall inform the CySEC in advance by defining the methods to be used and by submitting the standardized attestation.
      (iv) The use of such innovative methods takes place in accordance with the relevant best practices and guidelines published by the CySEC.
      (v) The Company must ensure that documentation, data and information gathered during the Client on-boarding process through innovative solutions remain accurate and up to date.
      (vi) The Company shall be responsible to set an explicit limit on the level of assets to be deposited and the size of transactions involved in order to be able to use an innovative identification method. Such limit is expected to vary per risk category and on a case-by-case basis, depending on the particular risks involved and on whether a combination of Innovative Client due diligence methods were used or were complemented with non-innovative/non-electronic Client due diligence methods.
      (vii) The persons within the Company that are responsible for the selection, including the documented justification in the risk assessment mentioned herein, implementation and monitoring of the Innovative Method(s), are the Board of Directors, the MLCO. The Internal Auditor will be responsible for independently auditing the risk assessment and the practical application of

the selected Innovative Method(s) and where deficiencies are identified to be immediately rectified.

b. Utilizing innovative methods or a combination of them as per the CySEC's Consultation Paper CP-02-2020. These methods may include without limitation the verification of the Client identity by taking a dynamic real time selfie, and/or a real time video call. The use of such methods shall be in line with the relevant best practices and guidelines published by CySEC.

c. Communicating with the Client through at an address that the Company has previously verified from an independent and reliable source, in the form of registered email e.g. direct mailing of account opening documentation, which the Client shall return to the Company or the sending of security codes required by the Client to access the accounts opened.

4. A true translation shall be attached in the case that the documents of point (1) above are in a language other than Greek of English.

Each time the Company shall proceed with the acceptance of a new Client, the Head Administration/Back Office Department shall be responsible for ensuring compliance with the provisions of points 1 and 2 above.

14.4. Data Protection, Record-Retention and Statistical Data

1. The processing of personal data under the Law is subject to the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018), as amended.

2. Personal data shall be processed by the Company on the basis of the Directive only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of the Directive for any other purposes, such as commercial purposes, shall be prohibited.

3. The Company shall provide new Clients with the information required pursuant to Paragraph 11(1) of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018), as amended, before establishing a business relationship or carrying out an occasional transaction. Also, the Company shall provide information to their new Clients before starting a business relationship or conducting an individual transaction for the processing of personal data under the Law for purposes of preventing money laundering and terrorist financing.

4. The right of access of the data subject to the data concerning him / her may be waived in part or in full according to the provisions of the Law providing for the Protection of Natural

Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018), as this has been amended from time to time:

(d) For the purposes of properly performing the duties of the Company , or
(e) In order not to impede the conduct of official or legal investigations, analyzes or proceedings for the purposes of the Law and to ensure that the prevention, investigation and detection of money laundering and terrorist financing.

5. The processing of personal data under this law for the purpose of preventing money laundering and terrorist financing is considered to be an issue of public interest in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the **"General Data Protection Regulation"**).

6. The Company incorporates strict rules and specific procedures into the day-to-day operations in order to guarantee its clients and employees the maximum achievable level of security in handling personal data. All personal data held by the Company is protected under the applicable Data Protection Legislation and the Data Protection Officer is responsible for overseeing the procedures and policies implemented by the Company for the processing of the personal data.

   Additionally, the Company ensures that the following data subjects' rights, as these are stated under the applicable Data Protection Legislation, are respected:

   - Request access to personal information which enables the date subject to receive a copy of his personal information that the Company holds about him and to check that the Company lawfully processing it.
   - Request correction of his personal information which enables the data subject to have any incomplete or inaccurate information corrected.
   - Request erasure of his personal information which enables the data subject to delete or remove personal information where there is no good reason for the Company continuing to process it.
   - Object to processing of his personal information where the Company is relying on a legitimate interest (or those of a third party) and there is something about his particular situation which makes him want to object to processing on this ground. The data subject has also the right to object where the Company is processing his personal information for direct marketing purposes.
   - Request the restriction of processing of his personal information which enables him to ask the Company to suspend the processing of personal information about him.
   - Request the transfer of his personal information to another party.

15. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

15.1. Employees' Obligations

(a) The Company's employees shall be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing
(b) the employees must cooperate and report, without delay, according to point (e) of Section 6.2, anything that comes to their attention in relation to transactions or any activity in a Client's accounts for which there is a slight suspicion that are related to money laundering or terrorist financing
(c) according to the Law, the Company's employees shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

15.2. Education and Training

15.2.1. Employees' Education and Training Policy

(a) The MLCO shall ensure that its employees are fully aware of their legal obligations according to the Law and the Directive, by introducing a complete ongoing education and training program of their employees' in the recognition and handling of transactions and activities which may be related to Money Laundering or Terrorist Financing.
(b) the timing and content of the training provided to the employees of the various departments will be determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system of the Republic
(c) the training program aims at educating the Company's employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose
(d) the training program aims also at educating the Company's employees on the relevant and latest requirements in relation to the protection of personal data,
(e) the training program will have a different structure for new employees, existing employees and for different departments of the Company according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The MLCO shall be responsible to refer to the relevant details and information in his/her Annual Report in respect of the employees' education and training program undertaken each year.

When setting up a staff training, the MLCO shall consider:

a. which staff require training
b. what is the content of the training provided; (e.g., legal framework, transactions monitoring, procedures for reporting suspicious transactions/activities, typologies/case studies of suspicious activities etc.)
c. what form the training will take
d. how often training should take place
e. how staff will be kept up to date with emerging risk factors for the regulated entity.

Further to the above, training can take many forms and may include:

a. face-to-face training seminars
b. completion of online training sessions
c. attendance at AML/CFT conferences and participation in dedicated AML/CFT forums
d. practice group meetings for discussion of AML/CFT issues and risk factors
e. guidance notes, newsletters, and publications on current AML/CFT issues.

Training must be provided to staff prior to commencing work on behalf of the Company, and after that, at a minimum on an annual basis, ensuring the delivery of regular training and updates as required.

15.2.2. MLCO Education and Training Program

The *Senior Management* of the Company shall be responsible for the MLCO of the Company to attend external training. Based on his/her training, the MLCO will then provide training to the employees of the Company further to Section 15.2.1 above.

The person to be appointed as MLCO and Assistant MLCO must possess the relevant certification mentioned in subparagraph 5.5 of the CySEC Directive regarding the Certification of Persons and the Certification Registers, as this has been amended from time to time (the **"Certification Directive"**).

The main purpose of the MLCO training is to ensure that relevant employee(s) become aware of:

- the Law and the Directive
- the Company's Anti-Money Laundering Policy
- the statutory obligations of the Company to report suspicious transactions
- the employees own personal obligation to refrain from activity that would result in money laundering
- internal AML/CFT policies and procedures
- any unique AML/CTF risks the Company may face
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

The MLCO shall be responsible to include information in respect of his/her education and training program(s) attended during the year in his/her Annual Report.

For the determination of the AML Training program, the following factors are taken into consideration:

a. the content of the training (i.e., legal framework, transactions monitoring, procedures for reporting suspicious transactions/activities, typologies/case studies of suspicious activities)
b. the frequency of the training
c. the form of the training
d. the way of keeping up to date the Company's personnel in respect to the emerging risk factors
e. number of training hours by type of employees and by type of department/function and percentage of employees having completed the training
f. whether the lecture/seminar will be prepared within the financial sector operator or offered by an external organisation or consultants and
g. summary information for the program/content of the lectures/seminars.

Further to the above, in case the Company outsource certain training activities to a third party, the Compliance Officer should ensure and document within the activity report the following:

a. the subcontractor has the required AML/CFT knowledge to guarantee the quality of the training to be provided,
b. the management conditions of the outsourcing are set and respected, and
c. the content of this training is adapted to the specific features of the financial sector operator concerned and that the field experience of the financial sector operator's AML/CFT compliance officer is properly reflected in the training.

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name: ..... Tel: .....

Department: ..... Fax: .....

Position: .....

CLIENT'S DETAILS

Name: ....

Address: ....

..... Date of Birth: .....

Tel: ..... Occupation:.....

Fax: ..... Details of Employer: .....

.....

Passport No.: ..... Nationality: .....

ID Card No.: ..... Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction: ....

....

Reason(s) for suspicion:..... .....
....

Informer's Signature Date

....

FOR MLCO USE

Date Received: ..... Time Received: ..... Ref. .....

Reported to the Unit: Yes/No .... Date Reported: ..... Ref .....

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: ..... Client's Details: .....

Informer: ..... Department: .....

INQUIRIES UNDERTAKEN (Brief Description)

.....

.....

.....

ATTACHED DOCUMENTS

.....

.....

.....

.....

MLCO DECISION

.....

.....

.....

FILE NUMBER .....

MLCO SIGNATURE DATE

....

EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING

A. MONEY LAUNDERING

1. Transactions with no discernible purpose or are unnecessarily complex.

2. Use of foreign accounts of companies or group of companies with complicated ownership structure which is not justified based on the needs and economic profile of the Client.

3. The transactions or the size of the transactions requested by the Client do not comply with his usual practice and business activity.

4. Large volume of transactions and/or money deposited or credited into, an account when the nature of the Client's business activities would not appear to justify such activity.

5. The Business Relationship involves only one transaction or it has a short duration.

6. There is no visible justification for a Client using the services of a particular financial organisation. For example the Client is situated far away from the particular financial organisation and in a place where he could be provided services by another financial organisation.

7. There are frequent transactions in the same financial instrument without obvious reason and in conditions that appear unusual (churning).

8. There are frequent small purchases of a particular financial instrument by a Client who settles in cash, and then the total number of the financial instrument is sold in one transaction with settlement in cash or with the proceeds being transferred, with the Client's instructions, in an account other than his usual account.

9. Any transaction the nature, size or frequency appear to be unusual, e.g. cancellation of an order, particularly after the deposit of the consideration.

10. Transactions which are not in line with the conditions prevailing in the market, in relation, particularly, with the size of the order and the frequency.

11. The settlement of any transaction but mainly large transactions, in cash.

12. Settlement of the transaction by a third person which is different than the Client which gave the order.

13. Instructions of payment to a third person that does not seem to be related with the instructor.

14. Transfer of funds to and from countries or geographical areas which do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.

15. A Client is reluctant to provide complete information when establishes a Business Relationship about the nature and purpose of its business activities, anticipated account

activity, prior relationships with financial organisations, names of its officers and directors, or information on its business location. The Client usually provides minimum or misleading information that is difficult or expensive for the financial organisation to verify.

16. A Client provides unusual or suspicious identification documents that cannot be readily verified.

17. A Client's home/business telephone is disconnected.

18. A Client that makes frequent or large transactions and has no record of past or present employment experience.

19. Difficulties or delays on the submission of the financial statements or other identification documents, of a Client/legal person.

20. A Client who has been introduced by a foreign financial organisation, or by a third person whose countries or geographical areas of origin do not apply or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.

21. Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g. student, unemployed, self-employed, etc).

22. The stated occupation of the Client is not commensurate with the level or size of the executed transactions.

23. Financial transactions from non-profit or charitable organisations for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction.

24. Unexplained inconsistencies arising during the process of identifying and verifying the Client (e.g. previous or current country of residence, country of issue of the passport, countries visited according to the passport, documents furnished to confirm name, address and date of birth etc).

25. Complex trust or nominee network.

26. Transactions or company structures established or working with an unneeded commercial way, e.g. companies with bearer shares or bearer financial instruments or use of a postal box.

27. Use of general nominee documents in a way that restricts the control exercised by the company's board of directors.

28. Changes in the lifestyle of employees of the financial organisation, e.g. luxurious way of life or avoiding being out of office due to holidays.

29. Changes the performance and the behaviour of the employees of the financial organisation.

B. TERRORIST FINANCING

1. Sources and methods

The funding of terrorist organisations is made from both legal and illegal revenue generating activities. Criminal activities generating such proceeds include kidnappings (requiring ransom), extortion (demanding "protection" money), smuggling, thefts, robbery and narcotics trafficking. Legal fund raising methods used by terrorist groups include:

i. collection of membership dues and/or subscriptions

ii. sale of books and other publications

iii. cultural and social events

iv. donations

v. community solicitations and fund raising appeals.

Funds obtained from illegal sources are laundered by terrorist groups by the same methods used by criminal groups. These include cash smuggling by couriers or bulk cash shipments, structured deposits to or withdrawals from bank accounts, purchases of financial instruments, wire transfers by using "straw men", false identities, front and shell companies as well as nominees from among their close family members, friends and associates.

2. Non-profit organisations

Non–profit and charitable organisations are also used by terrorist groups as a means of raising funds and/or serving as cover for transferring funds in support of terrorist acts. The potential misuse of non-profit and charitable organisations can be made in the following ways:

i. Establishing a non-profit organisation with a specific charitable purpose but which actually exists only to channel funds to a terrorist organisation.

ii. A non-profit organisation with a legitimate humanitarian or charitable purpose is infiltrated by terrorists who divert funds collected for an ostensibly legitimate charitable purpose for the support of a terrorist group.

iii. The non-profit organisation serves as an intermediary or cover for the movement of funds on an international basis.

iv. The non-profit organisation provides administrative support to the terrorist movement.

Unusual characteristics of non-profit organisations indicating that they may be used for an unlawful purpose are the following:

i. Inconsistencies between the apparent sources and amount of funds raised or moved.

ii. A mismatch between the type and size of financial transactions and the stated purpose and activity of the non-profit organisation.

iii. A sudden increase in the frequency and amounts of financial transactions for the account of a non-profit organisation.

iv. Large and unexplained cash transactions by non-profit organisations.

v. The absence of contributions from donors located within the country of origin of the non-profit organisation.