DXA Capital Investment Services S.A.

Prevention of Money Laundering and Terrorist Financing Policy

Contents

Chapter 1: General Definitions

For the purposes of this Policy, unless the context shall prescribe otherwise with alphabetical order:

"**Authority**" means the Authority for Combating Money Laundering which was established under article 7 of law 3691/2008 and operates under Article 47-51 of the Law and any applicable presidential decree referring to the operation of the Authority.

"**Basic Offences**" means the offences defined in Article 4 of the Law and specifically:

a) The criminal organization under Article 187 of the Penal Code (PC, Law No. 4619/2019, A' 95),

b) Terrorist acts, terrorist organization, and the punishable support and financing thereof under Articles 187A, 187B PC and 32 to 35 of Law No. 4689/2020 (A' 103),

c) Bribery and corruption of political figures and judicial officials under Articles 159, 159A, and 237 PC and bribery and corruption of public officials under Articles 235 and 236 PC,

d) Influence peddling and bribery and corruption in the private sector under Articles 237A and 396 PC and bribery - corruption for match-fixing under Article 132 of Law No. 2725/1999 (A' 121),

e) Crimes against telecommunications under paragraphs 1 to 4 of Article 292A, Articles 292B, 292C, 292D, and paragraphs 1 and 2 of Article 292E PC and illegal access to information systems or data under Articles 370A, 370B, 370C, paragraphs 2 and 3 of Article 370D, and Article 370E PC,

f) Intentional homicide under Article 299 PC, grievous bodily harm under Article 310 PC, fatal bodily harm under Article 311 PC, kidnapping under Article 322 PC, human trafficking under Article 323A PC, abduction of minors under Article 324 PC, and illegal detention under Article 325 PC,

g) Counterfeiting of currency and other means of payment under Article 207 PC, circulation of counterfeit currency and other means of payment under Article 208 PC, excessive currency manufacturing under Article 208A PC, counterfeiting and misuse of marks under paragraph 1 of Article 208G PC, preparatory acts under Article 211 PC, counterfeiting under Article 216 PC, distinguished counterfeiting of certificates under paragraph 3 of Article 217 PC, theft under Article 372 PC, distinguished theft under Article 374 PC, embezzlement under Article 375 PC, robbery under Article 380 PC, extortion under Article 385 PC, fraud under Article 386 PC, computer fraud under Article 386A PC, fraud regarding subsidies under Article 386B PC, treason under Article 390 PC, acceptance and disposal of crime proceeds under paragraph 1 of Article 394 PC, distinguished acceptance and disposal of crime proceeds under paragraph 2 of Article 394A PC, and usury under Article 404 PC,

h) Facilitation of offenses against minors under Article 348 PC, child pornography under Article 348A PC, enticing children for sexual purposes under Article 348B PC, child pornography representations under Article 348C PC, procuring under Article 349 PC, sexual intercourse with a minor for payment under Article 351A PC,

i) Offenses under Articles 20 to 23 of Law No. 4139/2013 (A' 74) regarding addictive substances,

j) Offenses under Articles 6, 15, and 17 of Law No. 2168/1993 (A' 147) regarding weapons, ammunition, explosives, and explosive devices,

ja) Offenses under Articles 53, 54, 55, 61, and 63 of Law No. 3028/2002 (A' 153) regarding the protection of antiquities and cultural heritage,

jb) Offenses under paragraphs 1 and 3 of Article 8 of Presidential Decree No. 181/1974 (A' 347) regarding protection from ionizing radiation,

jc) Offenses under paragraphs 5 to 8 of Article 29 and Article 30 of Law No. 4251/2014 (A' 80) regarding migration and social integration,

jd) Offenses for the criminal protection of the economic interests of the European Union under Article 24 of Law No. 4689/2020 (A' 103),

je) Stock market crimes under Articles 28 to 31 of Law No. 4443/2016 (A' 232),

jf) Offenses:

jf1) Tax evasion under Article 66 of Law No. 4174/2013 (A' 170) except for the first paragraph of paragraph 5, and cross-border fraud related to Value Added Tax (VAT) under Article 23 of Law No. 4689/2020,

jf2) Smuggling under Articles 155 to 157 of Law No. 2960/2001 (A' 265),

jf3) Offenses under paragraphs 1 to 3 of Article 28 of Law No. 1650/1986 (A' 160) regarding environmental protection and paragraphs 1 to 5 of Article 6 of Law No. 4037/2012 (A' 10) on marine pollution and the first subsection of paragraph 1 of Article 13 of Law No. 743/1977 (A' 319), as codified in a unified text by Presidential Decree No. 55/1998 (A' 58) regarding protection of the marine environment,

jf4) Offenses under Article 66 of Law No. 2121/1993 (A' 25) regarding intellectual property and paragraphs 1 and 2 of Article 45 of Law No. 4679/2020 (A' 71) regarding trademarks,

jg) Piracy under Article 215 of Presidential Decree No. 187/1973 (A' 261),

k) Offenses of non-payment of debts to the State under Article 25 of Law No. 1882/1990 (A' 43), except for subsection a' of paragraph 1, as well as non-payment of debts arising from fines or penalties imposed by courts or administrative and other authorities, and

ka) Any other offense punishable by imprisonment, with a minimum term of more than three (3) months, from which financial benefit arises.

In the true sense of paragraph jf) of Article 4 of Law No. 4557/2018 (A' 139), as amended by Article 3 of Law No. 4734/2020 (A' 196), "basic offenses" under Law No. 4557/2018 include all offenses from which financial benefit arises and which are punishable by imprisonment.

“**Beneficial Owner**” means the natural person(s) who ultimately owns or controls a Client or legal person or legal entity, the person(s) on whose behalf a transaction is being conducted, or the person who ultimately controls a legal person or entity. “Beneficial owner” shall mean in particular:

a) in the case of corporate entities: i) the natural person(s) who ultimately owns or controls a corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or other ownership interests in that entity, including through bearer shareholdings, or through control via other means. A shareholding of 25% plus one share or an ownership interest of more than 25% in the corporate entity held by a natural person shall be an indication of direct control. 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 control. Control through other means may be determined, inter alia, in accordance with the conditions of Article 32(2) to (5) of Law No. 4308/2014. The abovementioned do not apply to companies listed on a regulated market that are subject to disclosure requirements in accordance with European Union law

or equivalent international standards ensuring sufficient transparency regarding the beneficial owner, ii) the natural person(s) who hold the position of senior managing official if, and only if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified as the beneficial owner, or if there is any doubt that the person identified is the beneficial owner; the Company shall keep records of the actions taken in order to identify the beneficial ownership in accordance with the above.

b) in the case of trusts: i) the settlor(s), ii) the trustee(s), iii) the protector(s), if any, iv) the beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates, v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means.

c) in the case of other legal entities or legal arrangements similar to trusts, the natural person(s) holding equivalent or similar positions to those referred to in point (b).

(d) in relation the legal entities of public sector, beneficial owner is the physical person(s) that hold senior management position.

"**Business Relationship**" means a business, professional or commercial relationship 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.

"**Centralised Automated Mechanism of Electronic Retrieval of Data**" means as described in article 21A of the Law the automatedcentralised mechanism of electronic retrieval of data-system of banking accounts and payments account registry of article 62 of the law 4170/2013 which can identify the holders or administrators of -inter alia- banking accounts with their IBAN, data and information for physical or legal entities collected by the credit institutions of law 4261/2014, payment institutions and e-money institutions, foreign branches in the Republic, which operate in the Republic,

"**Central Registry of Beneficial Owners**" is the central registry of beneficial owners of corporate or other legal entities, as defined in article 20 of the AML Law.

"**Client**" or "**Client**" means any legal or physical person aiming to conclude a Business Relationship or conduct an Occasional Transaction with the Company.

"**Company**" means the obliged financial institution under the meaning of article 5 of the Law with the corporate name DXA Capital Investment Services S.A., incorporated in the Hellenic Republic and having its registered address at 23, Rigillis str., 10674 Athens, Greece with a corporate registration number in the General Commercial Registry 173460001000 and licensed by the Hellenic Capital Markets Commission with registration number 2/997/5.10.2023.

"**EBA**" means the European Banking Authority.

"**EIOPA**" means the European Insurance and Occupational Pension Authority.

"**ESMA**" means the European Securities and Markets Authority.

"**ESA Risk Factors Guidelines**" means the EBA/GL/2021/02 Joint Guidelines of EBA, ESMA and EIOPA under Articles 17 and 18(4) of the EU AML 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 or/and occasional transactions.

"**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 AML Directive**" means the Directive 2015/849/EE on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, which was amended by Directive 2018/843 of the European Parliament and of the Council of 30 May 2018, and as currently in force, and also as supplemented by Directive (EU) 2018/1673 on combating money laundering by criminal law.

"**EU MiFID II Directive**" means the 2014/65/EU Directive of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61, as in force.

"**Financial Intelligence Unit (FIU)**" means for Greece the unit of the Authority as set forth in Article 47 of the Law and for the other Member States the competent Unit for the prevention, detection and effective treatment of money laundering and terrorist financing.

"**GEMH**" is the General Commercial Registry of legal entities in the Hellenic Republic.

"**HCMC**" means the Hellenic Capital Markets Commission which is under article 6 of the Law the competent authority for the application of the Law regarding the obliged financial institutions whereas the Company is included.

"**HCMC Decisions**" means the HCMC Decisions that have been issued according to the authorization of law 2331/1995 (Government Gazette 173) and law 3691/2008 (Government Gazette A΄166) regarding the prevention of the use of the financial system for the purposes of money laundering and terrorist financing until they will be amended or abolished and as long as they are not contradictory to the provisions of the Law (as provided in par. 2 of article 53 of the Law) and any other HCMC Decisions that are issued from time to time.

"**HCMC Circulars**" are the circulars issued by the HCMC from time to time and they refer inter alia to the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

"**High-risk third country**" means a country identified by the European Commission as high-risk third country for money laundering or terrorist financing.

"**Investment services and activities and ancillary services**" means the investment services and activities and ancillary services as per Part I and Part II respectively of the First Appendix of the MiFID II Law under which the Company is licensed by the HCMC to offer the investment services/activities and ancillary services, as per presented under Section 3.

"**Laundering Offences**" (or money laundering offences) means under article 2 of the Law the following conducts, when committed intentionally: (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action; (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity; (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity; (d) use of the financial system by layering or transfer of profits that are derived from criminal activities in order these profits to be depicted as legal; (e)

participation in an organization or a team of at least two people for the activities referred in (a) - (d) above; (f) attempt to committing, aiding, abetting, facilitating or counselling any third person for committing one or more of the activities referred in (a) – (d) above of any of the actions referred to in points (a)- (d).

Laundering offence shall be regarded as such even where the activities which generated the assets to be laundered were carried out in another Member State or in a third country and this activity is illegal in such country and this activity would have been considered illegal if it was committed in the Republic.

"**Law**" or "**AML Law**" means law 4557/2018 as amended and in force for the Prevention and suppression of money laundering and terrorist financing (for the incorporation of 2015/849/EE Directive)and other provisions.

"**Policy**" means the present Prevention and suppression of money laundering and Terrorist Financing Policy of the Company.

"**MiFID II Law**" is the law 4514/2018, as in force, titled "On markets in financial instruments and other provisions" incorporating in the Greek legislation EU MiFID II Directive.

"**Occasional Transaction**" means any transaction that is not carried out in the course of an established Business Relationship formed by a person acting in the course of financial or other business.

"**Trust or company service provider**" means any person that, by way of its business, provides any of the following services to third parties:

(a) forming companies or other legal persons;

(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.

"**Politically Exposed Persons (PEPs)**" means within the meaning of points 9-11 of article 3 of the Law the natural persons who are or have been entrusted with prominent public functions in the Hellenic Republic or in another country and their immediate family members or persons known to be close associates of such persons.

"**Register of Beneficial Owners of Trusts**" means the registry of trusts under Article 21 of the AML Law.

"**Republic**" means the Hellenic Republic.

"**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 Title III of MiFID II Law , as in force, or EU MiFID II Directive.

"**Shell Bank**" means the credit institution or financial organization or foundation that engages in activities similar to those of credit institutions or financial organizations, which: a) is established in a country or jurisdiction where it does not have physical presence and therefore actual headquarters and management, and b) is not affiliated with a financial group that meets the requirements of Union legislation regarding the regulation and supervision thereof, or at least equivalent requirements..

"**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.

"**Unusual transaction or activity**" means under the meaning of article 3 par. 15 of the Law, par. 3 of article 16 of the Law and par. (56) of the ESA Risk Factor Guidelines, the Client's transaction or activity that is not in line with his transactional, business or professional activity or the ultimate beneficiary of the Client activity or is not in line with the Client's financial status or the transaction does not have an obvious scope or does not have a motive of a financial, business or personal nature. Unusual transactions may be under the meaning of par. (56) of the EBA Risk Factors Guidelines patterns or transactions that are large than the Company would normally expect based on its knowledge of the Client, the Business relationship or the category to which the Client belongs or/and transactions that have unusual or unexpected pattern compared with the Client's normal activity or the pattern of transactions associated with similar Clients, products or services or transactions that are very complex compared with other similar transactions associated with similar Client types, products or services.

Chapter 2: Introduction

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

The Policy is developed and periodically updated by the Anti Money Laundering Compliance Officer (hereinafter the "Compliance Officer") 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 Policy must be approved by the Board.

The Policy shall be communicated by the Compliance Officer to all the employees of the Company that manage, monitor or control in any way the Clients' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined herein and the Company's Internal Conduct of business Rules.

The Policy has been prepared to comply with the provisions of the Law, the HCMC Decisions and HCMC Circulars and any applicable national or European legislation.

Chapter 3: Policy Applicability

The Policy applies to all various types of investment services offered to the Company's Clients as well as the relevant Company's dealings with its Clients, irrespective of the Client account size and frequency of trading, according to the applicable legislation.

In this respect, the Compliance Officer shall be responsible to update the Policy so as to comply with the HCMC requirements, as applicable, regarding the Client identification and due diligence procedures which an investment firm must follow, for Clients whom the Company offers its investment services and ancillary services under its license issued by HCMC as follows:

		Investment services and activities									Ancillary services						
		1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7
Financial Instruments	1	✓	✓		✓	✓					✓	✓		✓	✓		
	2																
	3																
	4	✓	✓		✓	✓					✓	✓		✓	✓		
	5																
	6																
	7																
	8																
	9	✓	✓		✓	✓					✓	✓		✓	✓		
	10																
	11																

Chapter 4: Responsibilities of the board of directors

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 Compliance Officer and to the employees of the Company.

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 Compliance Officer and, where is necessary, assistant Compliance Officers and determine their duties and responsibilities, which are recorded in this Policy.

c) to approve the Policy and approve the updates when required.

d) where appropriate, enhance the measures adopted.

e) to ensure that all requirements of the Law and relevant HCMC Decisions and HCMC Circulars are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirements.

f) to ensure that the Compliance Officer 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 Back-Office Department), have complete and timely access to all data and information concerning Clients' identity and Client's verification documents and data, 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.

g) to ensure that all employees are aware of the person who has been assigned the duties of the Compliance Officer, as well as his assistants (if any), to whom they report, according to point (e) of Section 6.2 of the Policy any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing

h) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the Compliance Officer, in order the relevant actions to be taken under the Policy.

i) to ensure that the Compliance Officer, the assistant Compliance Officers, if any, and the Back-Office Department have sufficient resources, such as competent staff and technological equipment, for the effective discharge of their duties.

j) to assess and approve the Compliance Officer's Annual Report of Section 7 of the Policy and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report.

k) 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 Policy.

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

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

n) be informed of the results of the business-wide ML/TF risk assessment;

o) oversee and monitor the extent to which the AML/CFT policies and procedures are adequate and effective in light of the ML/TF risks to which the company is exposed and take appropriate steps to ensure remedial measures are taken where necessary;

p) at least once a year, review the activity report of the AML/CFT compliance officer and obtain interim updates more frequently for activities that expose the credit or financial institution to higher ML/TF risks;

Chapter 5: Obligations of the Internal Auditor

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 Policy.

(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.

Chapter 6: Compliance Officer

6.1. General

The Compliance Officer shall be appointed from the management ranks of the Company. Furthermore, the Compliance Officer shall lead the Company's Anti-Money Laundering Compliance procedures and processes and report to the Board. The Compliance Officer shall also have the resources, expertise as well as access to all relevant information necessary to perform his/her duties adequately and efficiently. The level of remuneration of the Compliance Officer shall not compromise his/her objectivity and will not be based on the examination he/she proceeds in the performance of the Company's Departments in the application of AML procedures.

In performing his/her role, the Compliance Officer considers 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.

6.2. Duties of the Compliance Officer

During the execution of his/her duties and the control of the compliance of the Company with the Law and the applicable legislation, the Compliance Officer shall obtain and utilise data, information and reports issued by international organisations, as these are stated in Chapter 8.5 of the Policy.

The duties of the Compliance Officer shall include, *inter alia* and in accordance with article 8 of the HCMC Decision 1/506/8.4.2009, the following:

(a) to design, based on the general policy principles of the Company mentioned in point (a) of Section 4 of the Policy, 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 Chapter 9 of the Policy, and submit it to the Board for consideration and approval and in general to implement the guidelines and broad instructions issued by the Board of Directors of the Company and create efficient and transparent processes to be followed across the Company, based on the said broad instructions and guidelines.

(c) to review and update the Policy 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 Chapter 4 of the Policy, the practices, measures, procedures and controls of point (a) above and in general the implementation of the Policy. In this respect, the Compliance Officer 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 Compliance Officer 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 of 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") signed from the relevant employee; a specimen of such report is attached in Appendix 1 of the Policy. The Compliance Officer may also receive information from other available sources and a relevant written report is made respectively.

(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 3 of the Policy.

- if following the evaluation described in point (f) above, the Compliance Officer decides to notify the FIU, then he should either fill in and submit the designated HCMC form which is available in the HCMC's website or to fill in and submit an online report (Suspicious Transactions Reports/Suspicious Activities Reports ("STR/SAR") on the web-application of the FIU and submit it through Electronic Report Submission System (https://estr.hellenic-fiu.gr/) the soonest possible.
- if following the evaluation described in point (f) above, the Compliance Officer decides not to notify the FIU then he should fully explain the reasons for such a decision on the Compliance Officer's Internal Evaluation Report.

(g) to act as a first point of contact with the FIU, upon commencement of and during an investigation as a result of filing a report to the FIU according to point (g) above, responding to any questions and clarifications requested from HCMC regarding the report and deciding if the questions and clarifications requested are related to the filing report and to this end grants all the appropriate information to the HCMC and fully cooperates with it.

(h) to ensure that the Back Office Department deals with 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 and termination of the Business Relationship and Occasional Transactions. Moreover, the Compliance Officer ensures that the Back Office Department proceeds in the updating of said list with all new or existing Clients, in light of any additional information obtained.

(i) 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 consult the Board of Directors for updating and amending the systems and procedures applied by the Company for the effective management of the aforesaid risks.

(j) to conclude under article 6 of no1/506/8.4.2009 HCMC Decision in written with a justified report that the prerequisites of Article 19 of the AML Law are fulfilled, if the Company relies on a third party for the verification of the identity of the Clients and its Beneficial owners.

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

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

(m) 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.

(n) to determine whether the Company's departments and employees need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organise appropriate training sessions/seminars. .

(o) to prepare the Annual Report according to Chapter 7 of the Policy and under par. 2 of Article 10 of the HCMC Decision 1/506/8.4.2009 which is completed electronically and submitted to the Board of Directors for approval.

(p) to respond to all requests and queries from the FIU and HCMC, provide all requested information and fully cooperate with them FIU.

(q) 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 of suspicious activity, date of submission to the Compliance Officer, date of assessment, date of reporting to the FIU), the evaluation reports of point (f) and all the documents that verify the accomplishment of his/her duties.

Chapter 7: Annual Report of the Compliance Officer

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

The Compliance Officer's Annual Report is prepared annually by filling in the questionnaire available on the hyperlink "Application for entering the data of the Annual Report", of the thematic section "Tackling money laundering" of the website of the Capital Market Commissionin accordance with par. 2 of article 10 of no 1/506/8.4.2009 HCMC Decision, and submitted to the Board for approval and upon approval is submitted within March of each year to the HCMC or the predetermined time pursuant to the relevant HCMC's Decisions.

Chapter 8: Risk-based approach

8.1. General Policy

The Company on the basis of the Law, the applicable HCMC Decisions and ESA Risk Factor Guidelines shall apply appropriate measures and procedures, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher. The Company shall assess and adjust -based on risk factors- the extent of its Client due diligence measures in a way that is commensurate to the money laundering/terrorist financing risk that has identified in order to mitigate the relevant risk. Determination of the risk factors, Client's assessment based on these risk factors at the establishment of the Business relationship, during the Business relationship and at the termination of the Business relationship and application of the proportionate measures to a Client upon the Company's assessment shall be the key elements for the adjustment of the risk-based approach in the Company's policies, practices and procedures. The Company shall obtain a holistic view. It will gather sufficient information to be satisfied that it has identified all relevant risk factors that may attach to a Client and where necessary apply enhanced due

diligence measures, and additionally will assess those risk factors to obtain a holistic view of the risk associated with a particular Business Relationship or Occasional transaction.

Further, the Compliance Officer shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of this Section of the Policy.

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

- recognises that the money laundering or terrorist financing threat varies across Clients, countries, services and financial instruments and distribution channels of services and financial instruments
- allows the Board to differentiate between Clients of the Company in a way that matches the risk of their particular business
- 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
- helps to produce a more cost-effective system
- 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.

The risk-based approach adopted by the Company and described in the Policy, 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:

- identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, financial instruments, services, distribution channels of services and financial instruments and geographical areas of operation of its Clients
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

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

Such indicators include the following:

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

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

The Compliance Officer shall be responsible for the development of the policies, procedures and controls on a risk-based approach. Further, the Compliance Officer shall also be responsible for the 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 Compliance Officer, at least annually, as per Chapter 5 of the Policy.

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 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 HCMC that the extent of measures and control procedures it applies are proportionate to the risk it faces regarding the Investment and Ancillary Services offered, 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 that are cash intensive

- PEPs
- Clients engaged in transactions which involves significant amounts of cash
- Client's or the beneficial owner businesses are commonly associated with higher corruption risk industry
- Client or the Beneficial Owner have links to sectors that are associated with higher money laundering and terrorist financing risk
- Client or the Beneficial Owner hold another prominent position or enjoy a high profile that enable the engagement to corruption
- Clients that are residents in countries of higher risk, i.e. countries):
    - identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
    - identified by credible sources as having significant levels of corruption or other criminal activity;
    - subject to sanctions, embargos or similar measures issued by, for example, the European Union or United Nations;
    - providing funding or support terrorist activities, or that have designated terrorist organisations operating within their country.
- In case that the Client is a legal person, is engaged or established in countries of higher risk, as defined above
- Clients convicted for a Basic Offence
- Client is a non-profit organisation or charity fund (or other form of philanthropic organisation of charitable nature) whose activities could be abused for terrorist financing purposes.

(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
- Client avoids the establishment of a business relationship, by carrying out one transaction or several one-off transactions
- Age of client or beneficial owner does not match with the type of services/products sought
- The sought products/services do not match with the Client's or beneficial owner's wealth situation
- Client requests unnecessary or unreasonable levels of secrecy.

(c) Risks based on the Company's products, services and the nature/means of communication with the client:

- services that allow payments from/to unknown or un-associated third persons/parties
- large cash deposits or withdrawals

- products or transactions which may favour anonymity (pre-paid cards, virtual or crypto-currencies et al)
- new products and business practises, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products
- non face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures
- Client has been introduced by a third party which is not part of the same group or its main business activity is unrelated to financial service provision
- Client has been introduced by a tied agent, that is without direct contract with the Company
- high levels of cross border business which create exposure to Terrorist Financing risk.
- Complexity of financial instruments offered
- Limited, increased or no international exposure of the Client

(d) Risks associated with geographic and jurisdictional factors

- The geographic position of the Client puts it at risk of being used as a transit station for people transporting assets for Terrorist Financing purposes.
- Bank deposits, investments, wire transfers, pre-paid cards of clients connected to focus jurisdictions (i.e. jurisdictions that present a higher risk of terrorism or which have strong geographical or other links with such countries) may pose a risk of Terrorist Financing for the Company.
- Persons associated with a client company (beneficial owners, relatives or associates of beneficial owners, persons exercising control over client company etc), which are from focus or high-risk jurisdictions may pose a risk of Terrorist Financing for the Company.
- Assets held or activities undertaken by clients in focus jurisdictions or linked to such jurisdictions; business relationships or one-off transactions with parties who are in or are linked to focus jurisdictions.
- The jurisdiction of the PEPs is not relevant in determining the type of PEP, but the domicile or nationality of the PEP is relevant to the risk. Foreign PEPs are always imposing higher risk than the domestic PEPs.

The Company shall collect information for assessing the Money Laundering and Terrorist Financing risk from a variety of sources, whether these are accessed individually or through commercial databases that pool information from several sources.

The Company shall always consider the following source of information:

- the European Commission's supranational risk assessment;
- information from government, such as the National Assessment of Money Laundering and Terrorist Financing Risks, policy statements and alerts, and explanatory memorandums to relevant legislation;

- information from the competent authorities, such as guidance and the reasoning set out in regulatory fines;
- information from Financial Intelligence Units (FIUs) and law enforcement agencies, such as threat reports, alerts and typologies; and
- information obtained as part of the initial Client due diligence process.

Other sources of information firms may consider in this context may include, among others:

- the Company's own knowledge and professional expertise;
- information from industry bodies, such as typologies and emerging risks;
- information from civil society, such as corruption indices and country reports;
- information from international standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists;
- information from credible and reliable open sources, such as reports in reputable newspapers;
- information from credible and reliable commercial organisations, such as risk and intelligence reports; and
- information from statistical organisations and academia.

The referred sources shall be used also for the implementation of Sections 10, 11 and 12 of the respective Policy.

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.
- obtaining tools and software which shall permit the proper identification of transactions, individuals, entities or jurisdictions which are subject to international sanctions.

- good understanding of Fintech, Regtech, block chain and other developing technologies and the way these might be offered or used for money laundering or terrorist financing purposes.

In this respect, it is the duty of the Compliance Officer 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 Chapters 9 and 10 of the Policy, respectively, as well as via a random sampling exercise as regards existing Clients.

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 Compliance Officer 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.

8.5. Relevant International Organisations

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 Compliance Officer shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force (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) - http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm

(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://esasjoint-committee.europa.eu/

(h) The Ministry of Foreign Affairs in relation to international sanctions by the UN Security Council, and restrictive measures of the Council of the EU http://www.mfa.gr/

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

Chapter 9: Client Acceptance Policy

The Client Acceptance Policy (hereinafter the "CAP"), following the principles and guidelines described in this Policy, 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 Compliance Officer shall be responsible for applying all the provisions of the CAP. In this respect, the Back Office Department shall also be assisting the AMLCO 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 Chapter 5 of the Policy.

9.1. General Principles of the CAP

The General Principles of the CAP are the following:

a) the Company shall classify Clients into three 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 Chapter 10 of the Manual

c) all documents and data described in Chapter 10.6 of the Policy must be collected before the establishment of a Business Relationship or an Occasional Transaction with a new Client

d) by way of derogation of point (c) above and according to Chapter 10.5(2) of the Policy, the verification of the identity of a new Client may be completed during the establishment of the business relationship

As per the remote electronic identification of Clients when registering on the Company's website (onboarding process), if the necessary documents under (c) are not provided at the time of entering into the business relationship, then the account on the Company's electronic trading platform will be opened without the possibility of conducting transactions (HCMC Decision 4/894/23.10.2020). Until all the necessary documents are submitted, the account will function as a "Demo Account".

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

This Section of the Policy 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 10.8 of the Policy.

For Low risk Clients, the Company will update their files every 3 years.

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 Policy are followed.

For normal risk Clients, the Company will update their file every 2 years.

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 Policy are followed.

Moreover, the Company shall apply the Enhanced Client Identification and Due Diligence measures for high risk Clients, according to Section 0.9 of the Policy.

For High risk Clients, the Company will update their file every year.

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 (see also Section 10.4 of the Policy)
- Shell Banks
- Clients included in Sanctions Lists
- Clients convicted for a Basic Offence
- Account(s) opened in anonymous or fictitious names(s)
- Account(s) for which the prospective Client is not approved by the Company.

9.4. Client Categorisation Criteria

This Section defines the criteria for the categorisation of Clients based on their risk. The Company 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 Company may apply simplified due diligence to Clients categorised as low risk based on the assessment of a non-exhaustive list of factors and types of evidence of potentially lower risk referred to in par. 2 of Article 15 of the Law and Annex I of the Law as below:

(1) Client risk factors:

(a) companies listed on a stock exchange which operates in EU or to other country that has compatible legislation with the EU Directive 2014/65 which impose requirements to ensure adequate transparency of beneficial ownership;

(b) public administrations or enterprises or EU organization or public international organization;

(c) Clients that are resident in geographical areas of lower risk as set out in paragraph (3);

(2) Product, service, transaction or delivery of products/services 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 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 limited by other factors such as small limits of transferred money or the transparency relating to the Client's identity

(3) Geographical risk factors/registration, legal seat, residency:

(a) Member States

(b) third countries identified by public international organizations as having a low level of corruption, organized crime or other criminal activity;

(c) 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.

It is provided that, further to the cases mentioned above, the Company has to gather sufficient information to establish that the Client qualifies as a low-risk Client. The information shall be duly documented and filed, as applicable, according to the recording keeping procedures described in Chapter 13.

9.4.2. Normal Risk Clients

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.

Clients can be classified as normal risk Clients with respect to the Money Laundering and Terrorist Financing risk which the Company faces applying Client due diligence measures in accordance with Article 13 of the Law and determining to what extent the measures described in par. 1 of the Law (see also Chapter 10.2 (a), (b), (c) and (d) of the Policy) shall be applied depending on the level of the risk which varies per Client on -inter alia- :

1. the purpose of the business relationship and the type of the Client
2. the type, frequency and value of the conducted transactions
3. professional activity and financial size of the Client
4. expected origin and destination of Client's funds
5. the offered investment services and the financial instruments that relate to the transactions

9.4.3. High Risk Clients

Clients can be classified as high-risk Clients based on the assessment of the following non-exhaustive list of factors and types of evidence of potentially higher risk referred to in par. 4 of Article 16 and Annex II of the Law as follows:

(1) Client risk factors:

(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) herein;

(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) a Client who is a national of a third country and applies for a right of residence or nationality in the Member State in exchange for transfers of capital, purchase of property or government bonds or investments in companies in that Member State.

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

(a) private banking;

(b) products or transactions that might favour anonymity;

(c) business relationships or transactions without the physical presence of the parties, without certain safeguards, such as electronic identification tools, relevant trust services

as defined in Regulation (EU) 910/2014 or any other secure, remote or electronic identification process that is regulated, recognized, approved or accepted by the relevant national authorities

(d) payment received from unknown or 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;

(f) transactions that are linked with oil, precious metals, smoking products, cultural items and other items of archeological, historical, cultural and religious importance or of rare scientific value as well as ivory and protected species.

(3) Geographical risk factors:

(a) countries identified by credible sources, other than the relevant EU acts, such as detailed assessment reports of public international organisations, as not having effective AML/CFT systems,

(b) countries identified by credible sources, such as detailed assessment reports of public international organisations, as having significant levels of corruption, organised crime or other criminal activity,

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

(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Chapter 10: Client Due Diligence and identification procedures

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

The Company under article 12 of the Law 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 Transactions that (i) amounts to Euro 15,000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked or (ii) constitutes a transfer of funds, as defined in point 9 of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (OJ L 141), exceeding 1,000 Euros,

(c) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction and regardless of any derogation, exception or minimum limit under the provisions of the Law

(d) when there are doubts about the veracity or adequacy of previous Client identification data or the ultimate beneficiary of the Client.

The abovementioned amounts are calculated without VAT or other legal withholdings that burden the Client.

In this respect, it is the duty of the Company to apply all the relevant Client Due Diligence Identification Procedures described in Section 10 of the Policy for the four (4) cases mentioned above. Furthermore, the Back-Office Department shall also be responsible to collect and file the relevant Client identification documents, according to the record keeping procedures described in Chapter 13 of the Policy.

Further, the Compliance Officer shall be responsible to maintain at all times template-checklists with respect to required documents and data from potential Clients, as per the requirements of the Law and the applicable legislation in order to be used from the Back-Office Department during the application of Client due diligence.

The Internal Auditor shall be responsible to review the adequate implementation of all the policies and procedures mentioned in Section 5.1 of the Policy, at least annually.

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

Client identification procedures and Client due diligence measures under article 13 of the Law shall comprise of:

(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 including, where available, electronic identification means, relevant trust services as set out in HCMC Decision 4/894/23.10.2020 relating to electronic identification and trust services for electronic transactions or any other secure, remote or electronic identification process regulated, recognised, approved or accepted by the relevant national authorities, in accordance with Decision no. 4/894/23.10.2020 of the HCMC on the remote electronic identification of natural persons, and the FATF Guidelines. When the Client acts through an authorized person, the Company identifies and verifies this person's ID, as well as his authorization documents.

(b) identifying the beneficial owner, updating the data and taking reasonable measures, as specified by decisions of the Hellenic Capital Market Commission. As regards legal persons, trusts or similar legal arrangements, reasonable measures are taken to understand the ownership and control structure of the Client, where the beneficial owner identified is the senior managing official, (as referred to in paragraph (a) (ii) of the definition term "Beneficial owner" within the Policy) shall take the necessary reasonable measures to verify the identity of the natural person who holds the position of senior managing official and shall keep records of the actions taken as well as any difficulties encountered during the verification process.

(c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship,

(d) conducting ongoing monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions or operations are consistent with the obliged person's knowledge of the Client, its business and risk profile, including, where necessary, the source of funds, according to

criteria that may be determined by the competent authorities. Furthermore, obliged persons ensure the keeping of up-to-date documents, data or information.

If the Company cannot comply with the abovementioned (a)-(c) Client due diligence requirements, it is obliged to deny the execution of the transaction, it does not establish a business relationship, or it terminates the Business Relationship and examines if exists an obligation of report to the FIU under Chapter 12 of the Policy.

The Company applies each of the Client due diligence measures and identification procedures set out above, but may determine the extent of such measures on a risk sensitive basis depending on

- the purpose of the business relationship and the type of the Client;
- the type, frequency and value of the conducted transactions;
- professional activity and financial size of the Client;
- expected origin and destination of Client's funds;
- the offered investment services and the financial instruments that relates to the transactions

The Company, additionally, is obliged under par. 3 (b) of article 13 of the Law to verify, when establishing a Business relationship, the annual assets of the Client based on the recent submitted to the tax authorities income tax statement, unless the Client is not obliged to submit an income tax statement or the transaction is not over ten thousand euros (10,000€), according to the applicable legislation. In case of joint accounts, securities or other financial products accounts, the beneficiaries of said accounts are considered as Clients and Client due diligence procedures are applied to them.

Any data and information collected from the clients shall be assessed based on the Section 8 of the Policy.

10.3. 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/her 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, in accordance with HCMC Decision no. 4/894/23.10.2020 on the remote electronic identification of natural persons and the FATF Guidelines.

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

Failure or refusal by a Client to submit, before the establishment of a Business Relationship or the execution of an Occasional Transaction, the requisite data and information for the verification of his/her identity and the creation of his/her economic profile (see Section 10.6 of

the Policy), 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 (see Section 9.3 of the Policy) while at the same time the Compliance Officer considers whether it is justified under the circumstances to submit a report to the FIU, according to point (g) of Section 6.2 of the Policy.

If, 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 Policy, the Company and the Compliance Officer shall consider terminating 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 FIU, according to paragraph point (g) of Section 6.2 of the Policy.

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

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

1. The identification and verification of the relevant data of the Client and the beneficial owner and other person(s) on whose behalf the Client is acting, takes place before the establishment of a Business Relationship or the carrying out of a transaction.Whenever entering into a new business relationship with a corporate or other legal entity, or a trust or a legal arrangement having a structure or functions similar to trusts ("similar legal arrangement") which are subject to the registration of beneficial ownership information pursuant to Article 20 and 21 of the AML Law i.e. the Central Registry of Beneficial Owners and the Register of Beneficial Owners of Trusts respectively the Company collects proof of registration;
2. By way of derogation from paragraph 1, the verification of the identity of the persons referred to in paragraph 1 above, could be allowed to 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. In such situations, the verification procedures are completed as soon as possible after the initial contact.
3. By way of derogation of point (1) above, it is possible to open an account with the Company, including accounts that permit transactions in transferable securities, provided that there 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 and identification procedures, as mentioned in Section 10.2 of the Policy.
4. Client due diligence measures shall be applied not only to all new Clients but also to existing Clients at appropriate times depending the level of Client's risk or when the relevant circumstances of a Client changes i.e. indicatively when one of the events or incidents referred in Section 10.7 (3) and points (b) to (d) of Section 10.1 of the Policy occur or when

the Company has any legal duty under the Law, the law 4172/2013 or the HCMC decisions in the course of the relevant calendar year to contact the Client for the purpose of reviewing any relevant information relating to the beneficial owner(s).

10.6. 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/her 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 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 nature/reason for requesting the establishment of a Business Relationship
   - the anticipated account turnover
   - the types of the transactions that could be executed
   - the banking account that the Clients funds will be returned
   - the Client's source and size of Client's assets and wealth and the description of 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)

These 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. 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) data and information that are used for the construction of the natural person's economic profile shall include inter alia the referred in point (a) to (e) above, the country of residency of the Client and in general, the same procedure regarding recording and update of these data/information as referred in point (f) above 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 Compliance Officer, according to point (e) of Section 6.2 of the Policy, and then by the latter to the FIU, according to point (g) of Section 6.2 of the Policy.

2. The Company shall apply for each of its Clients the above mentioned in par. 1 due diligence measures for the formation of the economic profile of the Client but may determine the extent of such measures on a risk-sensitive basis per Client or category of Clients.

The Company shall be able to demonstrate to HCMC that the extent of the measures is appropriate in view of the risks from the use of the Investment and Ancillary Services for the purposes of Money Laundering and Terrorist Financing.

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

(a) it is reasonably 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 the Law, that the Client is actually the person he claims to be.

In the case of remote identification, proof of identity is satisfactory if the natural person is participating live in the process and technological solution of the automated process without the

presence of an employee, by taking a dynamic-selfie in real time using a specialized software application, which is based on dynamic and not static capture photographs of the natural person (liveness), and it is verifiable that the characteristics of said person are matching the ones from the photos of the submitted documents.

The data and information collected for the construction of the economic profile shall be fully documented and filed, as applicable, by the Back-Office Department.

10.7. Further Obligations for Client Identification and Due Diligence Procedures

1. In addition to the principles described in Section 10.6. above, the Company, 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 maintains, especially those concerning high risk Clients.

Chapter 9.2.1- 9.2.3 of the Policy determines the timeframe during which the regular review, examination and update of the Client identification is conducted. The outcome of 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 Policy, 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.

3. In addition to the obligation of points (1) and (2) above, the Company shall check under the following occasions as inter alia included in par. 3 of article 16 of the Law and article 3 of 1/506/8.4.2009 HCMC Decision, the adequacy of the data and information of the Client's identity and economic profile, whenever indicatively one of the following events or incidents occurs:
   (a) an important transaction takes place which appears to be Unusual Transaction and/or of significant deviation 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.

In such cases, the Company enhances the level of monitoring of the business relationship in order to define if the relevant transactions are Unusual or Suspicious.

10.8. Simplified Client Identification and Due Diligence Procedures

The Company may apply simplified Client Identification and Due Diligence Procedures, provided that it will ensure that the business relationship or the transaction is of low risk.

In this respect, the Company ensures to collect sufficient information and perform monitoring of transactions in order to be able to conclude that the professional relationship or transaction is indeed of low risk and enable the detection of unusual or suspicious transactions.

When assessing the risks of money laundering, the Company takes into account at least the factors of potentially lower risk situations, as specified in Section 9.4.1 In particular the following shall apply:

1. For simplified Client Identification and Due Diligence Procedures, the Company may not verify the identification of the client or the beneficial owner, neither collect information regarding the purpose and the intended nature of the business relationship or perform verification of the identity of the Client and the beneficial owner after the establishment of the Business Relationship or the execution of an Occasional Transaction. Nevertheless, the Company will carry out background checks on the client to ensure that the risk of money laundering and terrorist financing is indeed lower. However, the Company under article 4 of HCMC Decision 1/506/8.4.2009 must collect at least the info ID of the legal representatives and the authorized persons who operate the Client's account as well as the resolution minutes of the competent body of the Client- entity for the legal representation and the operation of the account.
2. In addition to the above, the Company must exercise continuous monitoring of the business relationships mentioned in Section 9.4.1. according to the provisions of the paragraph (d) of Section 11.2. or report to the Unit any suspicious transaction or any attempt to carry out a suspicious transaction.
3. Further to the above, HCMC under par. 3 of article 15 of the AML Law may issue decisions in order to define low risk factors and measures that have to be applied in low risk business relationships or transactions. The Company will adopt accordingly.
4. It is provided that the Company shall collect sufficient information, so as to decide whether the Client can be exempted according to the provisions of point (1) - already mentioned in Section 9.4.1. The Company when assessing the abovementioned shall pay special attention to any activity of those Clients or to any type of transactions which may be regarded as

particularly likely, by its nature, to be used or abused for money laundering or terrorist financing purposes.

5. The Company shall not consider that Clients or transactions referred to in point (1) above represent a low risk of money laundering or terrorist financing if there is information available to suggest that the risk of money laundering or terrorist financing may not be low.

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

The Compliance Officer shall apply enhanced due diligence measures, in addition to the measures referred to in Sections 10.2, 10.5, 10.6 and 10.7 to Clients who have been assessed by the Company as high risk (refer to Section 9.4.3. of this Policy) and in the following cases mentioned below (10.9.1-10.9.3).

In case of a high-risk Client with an anticipated account turnover of more than 75.000 Euro, the Company is required to collect and verify the data and information referred in Section 10.10.1 based on documents certified by a public authority or a credit institution within the EU or a credit institution in another country that applies the FATF Recommendations.

10.9.1. High risk third countries

When the Company is transacting or establishes a business relationship with a natural person that is resident in a High-Risk Third country and/or with a legal entity established in a High Risk Third-Country.

With respect to business relationships or transactions involving High-Risk Third Countries, the Company shall apply the following enhanced Client due diligence measures:

i) obtaining additional information on the Client and on the Beneficial Owner(s), on the intended nature of the business relationship, on the source of funds and source of wealth of the Client and of the Beneficial Owner(s) as well as the reasons for the intended or performed transactions;

ii) obtaining the approval of senior management for establishing or continuing the business relationship;

iii) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

iv) ensuring, where applicable, that the first payment is carried out through an account in the Client's name with a credit institution subject to Client due diligence standards that are not less robust than those laid down in the Law.

In addition to the measures provided in point (iii) above, the Company shall apply, where applicable, one or more additional mitigating measures to persons and legal entities carrying out transactions involving High-Risk Third Countries. Those measures shall consist of one or more of the following:

(a) the application of additional elements of enhanced due diligence;

(b) the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;

(c) the limitation of business relationships or transactions with natural persons or legal entities from the High Risk third countries.

The Company does not automatically apply enhanced due diligence measures to the Client, in the case of branches or majority-owned subsidiaries located in high-risk third countries and owned by liable entities established in the European Union, when said branches or subsidiaries of majority participation fully comply with the policies and procedures applied at group level, in accordance with article 36 of the Law. In these cases, it adopts a risk-based approach.

10.9.2. Cross frontier corresponding banking relationships

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

i. gather sufficient information about the credit 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 thereon

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

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

iv. expressly define the respective responsibilities of each party in the framework of the correspondent agreement

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.

The Company shall not engage in or continue correspondent relationships with a shell bank or with a credit institution or financial institution that is known to allow its accounts to be used by a shell bank.

10.9.3. "Politically Exposed Persons" accounts

With respect to transactions or Business Relationships with PEPs, the Company shall:

i) establish appropriate risk management procedures for verifying whether the client is a politically exposed person. Such procedures may include, depending on the level of risk, the instalment of the reliable electronic data base for politically exposed persons, the research and collection of information from the client or publicly available information. In

case of legal entities and arrangements, the procedures aim to the verification of the political exposure of the ultimate beneficial owners, authorised signatories and persons duly authorised to act on half of the aforementioned. In such a case where one of the above is a politically exposed person, the account of the legal entity or arrangement is subject to the relevant procedures to be followed for a politically exposed natural person.

ii) have Senior Management approval for establishing Business Relationships with such Clients which is communicated to the Compliance Officer, as well as for the continuation of the business relationships with existing Clients which have become PEPs for which the Compliance Officer shall also be informed.

iii) take adequate measures to establish the economic profile of the client, including the source of wealth and source of funds. Evidence is regularly collected and renewed with respect to the nature and size of the client's transactions which are subject to regular monitoring.

iv) conduct enhanced on-going monitoring of the Business Relationship and reviewed on an annual basis with respect to its continuation.

Where a politically exposed person is no longer entrusted with a prominent public function by the Hellenic Republic or a member state or a third country, or with a prominent public function by an international organisation, the Company shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

The Company shall take into consideration the lists of PEPs that are publicly available according to paragraphs 4 and 5 of Article 18 of the Law.

10.10. Client Identification and Verification of Client's ID (Specific Cases)

The Company shall ensure that the necessary documents and information are properly collected regarding the following cases of Clients where required:

10.10.1. Natural persons residing in the Hellenic Republic or abroad, Legal entities established in the Hellenic Republic or abroad, Other legal persons/entities established in the Hellenic Republic or abroad

The minimum required information for the identification of Clients (natural persons, legal entities, other legal persons/entities without legal personality either in Greece or abroad) and the required documents for the verification of Client identity are as follows:

Details for Client Identification	Indicative Documents for Verification of Client Identity (Individual or Cumulative by Case)
NATURAL PERSONS – TABLE A	
✓ Full name and father's name ✓ Identification card number or passport number and issuing authority ✓ Date and place of birth	Either of: – Police Identification Card – Valid passport – Identification Card of those serving in Law Enforcement Agencies and Armed Forces
✓ Current residential address	Either of: – Recent Utility Bill (up to 3 months) – Lease Agreement deposited with a Public Financial Service or evidenced through taxis net (landlord/tenant acknowledgment) – Tax Clearance Certificate or other documents issued by the Tax Office – Residence Permit or valid Residency Document
✓ Contact phone number	Recent landline or mobile phone provider bill *(The Client's contact phone number, if it is mobile, can be registered and confirmed with a one-time password (OTP))*
✓ Occupation *(regardless of whether it is a private individual or a professional)*	Either of: – Employer Certification – Tax Clearance Certificate or other documents issued by the Tax Office – Copy of recent payslip – Professional Identification – Insurance Fund Document
✓ Tax Identification Number ✓ Source of income	– Tax Clearance Certificate or other documents issued by the Tax Office – Certificate of non-obligation to submit a tax return (in case there is no tax return)
LEGAL ENTITIES-– TABLE B	
1. SOCIETE ANONYME, PRIVATE COMPANIES & LTD	
✓ Company name,	Cumulatively:

✓ registered office, ✓ duration, ✓ purpose, ✓ names of the partners (for LTD, PC), ✓ names of company managers	– current codified Articles of Association *(GEMI announcement with the codified statute attached, or gazette with a summary of the statute and its subsequent amendments either in the gazette or in the GEMI)* – Certificate of good-standing (general certificate of GEMI (recent))
✓ Details of the members of the Board of Directors	Cumulatively: - GEMI announcement for SA Representation - GEMI representation certificate (either current or detailed) – recent
✓ Details of the Legal representatives of the Company and their identification details, ✓ as well as of any beneficial owners	The documents specified case by case in Table A
✓ Tax Identification Number	Tax Clearance Certificate or other documents issued by the Tax Office (for the legal entity)
2. PERSONAL COMPANIES (OE, EE)	
✓ Company name, ✓ registered office, ✓ duration, ✓ purpose, ✓ names of the partners and the company managers	Cumulatively: – current codified Articles of Association *(GEMI announcement with the codified statute attached, or gazette with a summary of the statute and its subsequent amendments either in the gazette or in the GEMI)* – Certificate of good-standing (general certificate of GEMI (recent))
✓ Details of the Legal representatives of the Company and their identification details, ✓ as well as any of any beneficial owners	The documents specified case by case in Table A

✓ Tax Identification Number	Tax Clearance Certificate or other documents issued by the Tax Office (for the legal entity)
3. OTHER LEGAL PERSONS OR FORMS OR ENTITIES WITHOUT LEGAL PERSONALITY	
✓ Company name, ✓ registered office, ✓ duration, ✓ purpose	Cumulatively: Copies of the required legal documents, as well as any amendments to them
✓ Details of the Legal representatives of the Company and their identification details, ✓ as well as any of any beneficial owners	The documents specified case by case in Table A
✓ Tax Identification Number	Tax Clearance Certificate or other documents issued by the Tax Office (for the legal entity)

In case the contracting party or counterparty acts on behalf of a Client (natural or legal person, or other legal entities/entities) besides providing proof of their own identity as defined above, the certification and verification of the Client's identity details according to the above-defined criteria are also required.

If the Client is a natural or legal person, entity, or formation from a foreign country regarding identity certification, the provisions in this article and tables apply accordingly.

As verification documents, any valid documents issued by the competent authorities of the Client's country of origin may be accepted, including certificates or documents from relevant authorities maintaining registries and data or other generally evidentiary documents according to the legislation of that country. The Company may request translation of the required documents to understand their content.

10.10.2. Joint Accounts

In cases of joint accounts held by two or more natural or legal persons, all account holders are considered Clients, and the due diligence procedures outlined in Chapter 10 and the Law are applied to them.

10.10.3. Clients with a total investment capital of less than 10,000 Euros

Specifically, for Clients with a total investment capital of less than 10,000 Euros, certification is required only for the following details listed in Table A of the aforementioned paragraph 10.10.1:

- Full name and father's name
- Identification card number or passport number and issuing authority
- Date and place of birth
- Current residential address
- Contact phone number
- Tax Registry Number

10.11 Reliance on Third Persons for Client Identification and Due Diligence Purposes

The Company may rely on third persons for the implementation of points (a), (b) and (c) of Section 10.2 of the Policy (i.e. with par. 1 of article 13 of the Law)

1. For the purposes of this Section of the Policy, third person means credit institutions, financial leasing companies, factoring companies, asset management companies, mutual funds companies, financial institutions, investment intermediaries' companies, insurance companies, e-money companies that have their legal seat in a member state or in a third country which is a member of FATF and has not been highlighted from the European Commission as at High Risk Third Country.
2. If the Company relies on a third party, then:
   (a) receives from the third party every information that the latter obtains by applying the Client's or/and Beneficial Owner/s due diligence under Chapter 10.2 (a), (b) and (c) of the Policy (also as described in par. 1 of Article 13 of the Law).
   (b) ensures that the third party makes immediately available all data and information upon the Company's request in copies, either hard copies of electronically, having applied the Client due diligence procedures including Client's ultimate beneficiary owner due diligence procedures (if such case applies), including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council relating to electronic identification and trust services for electronic transactions or any other secure, remote or electronic identification process that the third party has acquired during the application of the abovementioned Client due diligence.
3. The ultimate responsibility for meeting the abovementioned requirements of Client identification and due diligence shall remain with the Company.
4. The Company in case of reliance to third party/ies must comply with the 34/586/26.5.2011 HCMC Decision which requires:
   (a) the necessity of drafting and applying an internal Company's Third Party Reliance Policy or Procedure and Risk Management Plan which will describe inter alia the risk assessment of reliance in a third party, the factors that have to be taken into consideration for this risk assessment, existence of alternative third parties to provide

the service, time and cost in case of replacement of the third party, the due diligence process on qualitative and quantitative criteria that the Company follows for choosing a specific third party, measures to be implemented in case the third party does not execute its duties, continuous monitoring and assessment of the third party,

(b) the necessity of signing a contract with the third party which must include at least the elements referred in article 4 of the relevant HCMC Decision,

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

Chapter 11: On-going monitoring

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 FIU, according to point (g) of Chapter 6. par. 2, Chapter 12 of the Policy and articles 22 and 23 of the AML Law.

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 Compliance Officer 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.

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 (e.g. the Back Office Department) shall be responsible to communicate with the Compliance Officer

(b) further to point (a) above, the **investigation** of unusual or suspicious transactions by the Compliance Officer. 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:

i. adequate automated electronic management information systems which will be capable of supplying the Board of Directors and the Compliance Officer, 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 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

ii. automated electronic management information systems to extract data and information that is missing or has to be updated regarding the Client identification and the construction of a Client's economic profile.

iii. 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/her origin, the origin and 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 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.

In any event the Company shall ensure that the clients are obliged to inform immediately the Company, in case of any changes on the provided data and information.

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

Chapter 12: External Reporting

12.1. Reporting of Suspicious Transactions to the FIU

The Company, in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the Compliance Officer its suspicion to the FIU in accordance with point (g) of Section 6.2, Chapter 12 of the Policy and articles 22 and 23 of the Law.

12.2. 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 the Section B of no 49/2012 of HCMC Circular and no 41/2009 of HCMC Circular as per Appendix 3. 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 Compliance Officer and the 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 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. Suspicious transactions include also the attempted transactions which must be reported respectively.
3. In order to identify suspicious transactions, the Back Office Department 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 as mentioned above.

Furthermore, the Compliance Officer 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 according to point (e) of Section 6.2 of the Policy. These reports are archived by the Compliance Officer

- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchange 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 Compliance Officer is evaluated on the Internal Evaluation Report according to point (f) of Section 6.2 of the Policy, which is also filed in a relevant file
- if, as a result of the evaluation described above, the Compliance Officer decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU, according to point (g) of Section 6.2 and Section 12.4 of the Policy.
- if as a result of the evaluation described above, the Compliance Officer decides not to disclose the relevant information to the FIU, then he/she fully will explain the reasons for his/her decision in the Internal Evaluation Report.

12.3. Compliance Officer's Report to the FIU

All the reports of the Compliance Officer of point (g) of Section 6.2 of the Policy should be prepared according to the sample report which is available in the HCMC's website or online on the web-application of the FIU and submitted to it, through the Electronic Submission Reporting system.

Before the submission of a suspicion report of point (g) of Section 6.2 of the Policy, the Company refrains from carrying out transactions which knows or suspects to be related to proceeds of criminal activity or terrorist financing unless it is impossible or is likely to frustrate efforts to pursue the Client of a suspected operation and in such a case must inform the FIU afterwards. The Company exercises particular caution, not to alert the Client concerned that a suspicion report has been submitted to the FIU. Close liaison with the FIU is, therefore, maintained in an effort to avoid any frustration to the investigations conducted.

Additionally, after submitting the suspicion report of point (g) of Section 6.2 of the Policy, the Company adheres to any instructions given by the FIU and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

12.4. Submission of Information to the FIU

The Company shall ensure (see also Chapter 13 of the Policy) that in the case of a suspicious transaction investigation by the FIU, the Compliance Officer will be able to provide without delay inter alia 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:

i. the origin of the funds;

ii. the type and amount of the currency involved in the transaction;

iii. the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers

iv. the identity of the person that gave the order for the transaction;

v. the destination of the funds;

vi. the form of instructions and authorisation that have been given;

vii. the type and identifying number of any account involved in the transaction.

Chapter 13: Record-keeping procedures

13.1. General

The Compliance Officer along with the Back Office Department of the Company shall maintain records under the provisions of article 30 of the Law of:

(a) the documents and information which are necessary to comply with the due diligence requirements laid down in Article 13 of the Law (Chapter 10 of this Policy), including, where available, information obtained through electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the Hellenic Telecommunications and Post Commission (EETT), for a period of five years after the end of the business relationship with their Client or after the date of an occasional transaction.

(b) the originals or copies of the legal documents necessary for the identification of the transactions,

(c) the internal documents relating to authorisations or findings or proposals for cases relating to the investigation of the abovementioned offences or to cases reported or non-reported to the FIU,

(d) the details of the business, commercial and professional correspondence with Clients, as determined by the supervisory authorities.

The documents/data mentioned above, as well as the data accessible through the Central Electronic Data Search Mechanism of article 21A of the Law will be kept in printed or electronic form for a period of five (5) years from the termination of the transactional relationship with the Customer or from the date of each transaction. At the end of the above period, the Company will delete the personal data, unless it is allowed to keep them for longer periods (which cannot exceed ten years) according to another law or regulation.

The above information shall be kept in a manner that the Company may fully and without delay respond, through channels ensuring the confidentiality of the investigations, to any request of the FIU, the competent or other public authority as to whether it maintains or had concluded, in the last five (5) years, a professional relationship with specific persons, as to the type of the professional relationship and as to any related transaction.

13.2. Format of Records

The Compliance Officer along with the Back Office Department shall retain the documents/data mentioned in Section 13.1 of the Policy, preferably in electronic otherwise in physical form, provided that the Back Office Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to HCMC or to the FIU, after a relevant request.

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

Chapter 14: Employees' obligations, education and training

14.1. 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 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 or unusual transactions or activities regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

14.2. Education and Training

14.2.1. Employees' Education and Training Policy

(a) The Company shall ensure that its employees are fully aware of their legal obligations according to the Law and the applicable legislation, as well as internal policies and procedures including unique risks the Company may face, by introducing a complete employees' education and training program

(b) The employees shall receive training with regards to their legal obligation to report on any reasonable suspicion or knowledge that comes to their attention that another person is engaged in laundering or financing of terrorism offences. In such cases, employees are obliged to make an internal report to the Compliance Officer as per the provisions of 6.2 (e). Moreover, the employees shall receive ongoing training with regards to suspicious activity monitoring and reporting, and specifically with regards to

the recognition and handling of transactions and activities which may be related to money laundering or terrorist financing

(c) 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. Such content shall be reviewed and updated on a regular basis to ensure that it remains current and appropriate, and the material is approved by senior management. Enhanced training shall be provided to senior management and staff in key AML/FT roles. 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, including any relevant acts of the European Union

(d) Training may take many forms and may include face-to-face training seminars, completion of online training sessions, attendance at AML/FT conferences and participation in dedicated AML/FT forums, practice group meetings for discussion of AML/FT issues and risk factors, guidance notes, newsletters and publications on current AML/FT issues

(e) the training program aims at educating the Company's employees on the latest developments in the prevention and suppression of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose

(f) 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

(g) Training shall be provided to staff prior to commencing work and at minimum on an annual basis. The Company shall establish mechanisms to facilitate prompt updates on key trends, emerging risks, potential ML/TF activities/risks, legislative changes and internal policies, controls and procedures and shall ensure that such updates are communicated to staff in a timely manner.

The Compliance Officer 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. Training records shall be maintained.

14.2.2. Compliance Officer Education and Training Program

The *Senior Management* of the Company shall be responsible for the Compliance Officer of the Company to attend external training. Based on his/her training, the Compliance Officer will then provide training to the employees of the Company further to Section 14.2.1 above.

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

- the Law
- 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
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

The Compliance Officer 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.

APPENDIX 1 – Internal Suspicion Report (ISR)

INTERNAL SUSPICION REPORT

INFORMER'S DETAILS

Full Name:	
Position	
Department:	
E-mail:	
Telephone:	

CLIENT'S DETAILS

Full Name:	
CID:	
Address:	
Telephone:	
Date of Birth/ Date of Incorporation:	
Passport/ Company Number:	
ID Card:	
Nationality:	

SUSPICIOUS CIRCUMSTANCES

Description of activities/ transactions:
Reason(s) for suspicion (behaviour, Client's background; account activity):

Informer's Signature **Date**.....

For AML Compliance Officer use:

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

Ref.....

Compliance Officer Signature

APPENDIX 2 – Internal Evaluation Report (IER)

INTERNAL EVALUATION REPORT

Reference	
Client's details	
Informer:	
Department:	

Inquiries undertaken (Brief Description):
Attached Documents:
Compliance Officer Decision:
File Number:

Compliance Officer Signature

Date: .....

APPENDIX 3 – Typology of SARS

A suspicious transaction is generally considered one that can be deemed incompatible with the client's known and lawful activities or personal transactions, or with the usual business cycle of the specific account. Some examples of transactions that may be associated with an intention to legitimize income from criminal activities include:

- ☐ Unjustified delay or refusal by the client or their authorized representative to provide the necessary legal documents for opening an investment account, or a general unwillingness to provide comprehensive information regarding the nature of their business activities.
- ☐ Rumors and news concerning the client or individuals associated with them linking them to criminal and punishable activities. The company is obliged to immediately report when there are publications in the press regarding illegal activities of its clients.
- ☐ Opening an account for conducting securities transactions in the name of a client, natural or legal person, whose residence or place of work, or - in the case of a legal person - headquarters, is not in the area served by the specific branch.
- ☐ At the request of the Company, the client refuses or fails to certify the legal origin of the funds or portfolio, either the information provided is false or misleading.
- ☐ Client who has professional relationships or originates from or is based or has a bank account in non-cooperative countries or countries that do not adequately implement FATF recommendations.
- ☐ Client who has professional relationships or originates from or is based or has a bank account in drug-producing or trafficking countries.
- ☐ Provision of information by the client that is difficult to verify by the Company.
- ☐ Movement of accounts with large sums held in the name of offshore companies. Activation of dormant investment accounts for a long period.
- ☐ Significant and sudden increase in transactions relative to the client's investment profile.
- ☐ Unusual nervousness in the behavior of individuals during the transaction.
- ☐ Lack of reasonable interest shown by the client in the financial terms of the transaction.
- ☐ Client's refusal to have personal contact with the Company.
- ☐ Request from the client to transfer monetary amounts to investment or bank accounts of other clients with whom they are not connected by professional or familial ties (suspicious transaction also for terrorism financing).
- ☐ Request from a corporate client to transfer monetary amounts to investment or bank accounts of branches or subsidiaries in other countries (suspicious transaction also for terrorism financing).
- ☐ Repeated similar transactions for amounts slightly below the minimum threshold requiring due diligence measures.
- ☐ Frequent change of client's address not justified by their professional activity.
- ☐ Cases of clients whose living standards constantly change, as well as their appearance.

☐ Collaboration of the client with a large number of politically exposed persons (PEPs).

☐ Regular transfers of portfolios to and from other PEPs.

☐ Crediting of the client's investment account via deposits from multiple bank branches of one or more banks.

☐ Client's name not stated in the justification of a monetary deposit into the Company's bank account for crediting the investment account.

☐ Large number of individuals depositing sums into the same client's bank account without satisfactory explanation.

☐ Investment account of the client where handling authorization is granted to individuals who do not appear to have any relationship with the client (either familial or professional).

☐ Transfers to the client's bank account where co-beneficiaries do not seem to have any relationship with the client (either familial or professional).

☐ Common investment account of individuals who do not seem to have any relationship with each other (either professional or familial).

☐ Client's home or business phone is deactivated.

☐ Suspicion or discovery of establishing dummy businesses by the client.

☐ Conducting complex or unusual transactions without clear economic or legal reasons.

☐ Deposits of large sums in cash or checks at the Company's cashier or/and large withdrawals in cash or checks from the Company's cashier.

☐ Request for money transfer to the client's bank account following a recent deposit into the client's investment account without any previous transaction.

☐ During the verification and certification of the client's identity, inconsistency is observed among the submitted information, leading to questions about the validity of some of these details (e.g., differences in address, postal address, contact number, profession, place and date of birth, patronymic, Tax Identification Number, etc.).

☐ Clients who always insist on dealing with the same employee even for routine transactions or who stop dealing with the Company during the absence of a specific employee.

Suspicious transactions/activities possibly related to tax evasion:

☐ A client unwilling to provide the clearance certificate of their personal income tax declaration or the submitted income tax declaration of their legal entity as a prerequisite for the formation of their economic/transactional profile, despite repeated requests from the Company.

☐ There are external sources (local community, media, etc.) indicating that a client is involved in activities possibly related to tax evasion or that their lifestyle is disproportionately luxurious compared to the income declared in their tax declaration.

☐ Deposits are made into the investment account of a natural person client who is the owner of a company, which are not compatible with the reported income or the place of residence,

raising suspicions that these deposits may possibly be related to concealed sales of the company or other corporate events.

☐ Significant transactions are conducted in the investment account of a client for whom the Company has received requests from tax, customs, judicial, or prosecutorial authorities to provide information or impose provisional measures to safeguard public interests, or in investment accounts of their family members or close associates.

☐ The transactional activity of a client, for whom the Company has been informed of requests from tax, customs, judicial, or prosecutorial authorities to provide information or impose measures to safeguard public interests, is transferred to a new investment account belonging to the client, their family members, close associates, or a company owned, managed, or represented by them.

☐ Repeated investments are made in dividend-paying stocks to appear as income, without yielding any real economic benefit.

☐ Indications from the subsequent income tax declaration of the client that only profitable transaction items have been selectively used to declare increased tax-exempt income.

☐ Indications of employee behavior that may be considered suspicious and related to the intent to legitimize income from criminal activities:

- The employee leads an extravagant lifestyle that cannot be justified by their salary.
- The employee fails to comply with recognized policies, procedures, and methods of the Company.
- The employee is reluctant to take leave.
- Changes in the performance or behavior of the employee.