DMTECH CREDIT FUND LTD

PREVENTION OF MONEY LAUNDERING & TERRORIST FINANCING

MANUAL

May 2024

DMTECH CREDIT FUND LTD
AML/CFT & KYC PROCEDURES MANUAL
Accepting investments into technology startups from business angels and family offices (HNWI/UHNWI)

---

1. Introduction

This Manual sets out DMTECH CREDIT FUND LTD's internal practices, procedures and controls for preventing money laundering and terrorist financing, KYC and CFT. It is maintained by the MLCO and approved by the CEO.

2. General Definitions

(Select terms)

- **Beneficial Owner: Natural person(s) with ultimate ownership/control (>25% share or equivalent).**
- **Business Relationship: Any ongoing professional relationship with a Client.**
- **Client: Any individual or entity seeking to invest.**
- **EDD: Enhanced Due Diligence for high-risk Clients.**
- **SAR: Suspicious Activity Report filed with MOKAS.**

3. Responsibilities of the CEO

- **Approve AML/CFT policy and Manual**
- **Appoint MLCO and allocate sufficient resources**
- **Ensure systems detect and prevent money laundering arising from serious tax offenses**
- **Oversee annual training program**

4. Money Laundering Compliance Officer (MLCO)

- **Maintain and update this Manual**
- **Oversee onboarding, transaction monitoring, SAR filings**
- **Liaise with MOKAS and regulators**
- **Design risk-based policies and document internal controls**

5. Risk-Based Approach

- **Categorize Clients by risk factors (HNWI/UHNWI, PEP status, jurisdiction)**
- **Apply EDD for high-risk categories**
- **Sources: FATF, MONEYVAL, EU Sanctions Map, UN Security Council**

6. Client Acceptance Policy (CAP)

- **Preliminary risk assessment on every prospective Client**
- **Reject or escalate any application lacking satisfactory documentation**

7. Client Identification & Due Diligence

7.1 When to Apply

- **Onboarding a new Client**
- **`Any single transaction ≥ €15,000`**
- **Suspicious circumstances, regardless of amount**
- **Material change in Client profile**

7.2 Required Documentation

- **Individuals: Valid ID/passport, proof of address, source-of-fund declaration**
- **Entities: Certificate of incorporation, articles of association, ownership structure, director/beneficial-owner IDs**

7.3 Multi-Stage Automated Screening

All automated checks run after initial onboarding via Sumsub:

1. **Sumsub – sanctions (EU/UN/OFAC), PEP, adverse media, face-document biometric match**
2. **Cardamon – AI-driven extraction of regulatory obligations, policy-gap detection, remediation guidance**
3. **Vivox AI – AI-powered document authenticity and facial verification**
4. **Intrepid Fox – Deep-dive into corporate and trust structures to identify hidden UBOs**

7.4 Failure or Refusal

If a Client refuses or fails to provide required information, terminate the relationship and consider SAR filing.

7.5 Onboarding of High-Net-Worth Individuals (HNWI)

8. Ongoing Monitoring & KYC Updates

- **Annual re-screening of all Clients or upon major profile changes**
- **Real-time transaction monitoring with threshold and behavioral alerts**
- **Investigate and escalate within 24 hours**

9. Suspicious Activity Reporting

- **File a SAR with MOKAS promptly upon detecting suspicious behavior**
- **Retain SAR records for at least five years**

10. Sanctions Compliance

- **Weekly updates of EU/UN/OFAC lists via Sumsub; validate changes via Cardamon**
- **Immediately suspend/terminate any Client newly listed**

11. Data Retention & Protection

- **Retain all KYC and transaction records for minimum five years post-relationship**
- **Ensure GDPR compliance: encryption, access controls, secure storage**

12. Staff Training & Awareness

- **Mandatory annual AML/CFT training covering Sumsub, Cardamon, Vivox AI, Intrepid Fox**
- **Biannual tabletop exercises to validate response protocols**

References

1. **Sumsub – https://sumsub.com/about/**
2. **Cardamon – https://cardamon.ai/**
3. **Vivox AI – https://www.vivox.ai/ & https://app.vivox.ai/**
4. **Intrepid Fox – https://intrepidfox.ai/**

Conclusion:
By integrating Cardamon, Vivox AI, and Intrepid Fox following Sumsub's initial screening, DMTECH CREDIT FUND LTD ensures a fully automated, risk-based AML/CFT framework. This approach delivers rapid, comprehensive due diligence and ongoing monitoring that meets the unique needs of handling investments from high-net-worth and ultra-high-net-worth investors into technology startups.

1. GENERAL DEFINITIONS

For this Manual, unless the context shall prescribe otherwise:

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

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

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

   A shareholding of twenty-five percent plus one share (25% +1 share) or an ownership interest of more than twenty-five percent (25%) in the Client held by a natural person shall be an indication of direct ownership. A shareholding of twenty-five percent plus one share (25% + 1 share) or an ownership interest of more than twenty-five percent (25%) in the Client held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control.

   Control through other means may be determined, inter alia, following the criteria of Sections 142(1)(b) and 148 of the Companies Law (Cap.113), as applicable.

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

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

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

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

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

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

"Company" means **LAVALANE LTD** which is incorporated in the Republic of Cyprus with registration number **HE 387079**.

"Credit Institution" has the meaning given to the term in Article 4, Paragraph 1, Subparagraph 1 of the Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and firms and amending Regulation (EU) No 648/2012, and includes a credit institution to which a license to operate as an authorized credit

institution (ACI) pursuant to the provisions of the Business of Credit Institutions Law and a credit institution which operates in the Republic of Cyprus pursuant to provisions of Section 10A of the Business of Credit Institutions Law.

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

"Cryptocurrency" means a digital representation of a value that is not issued by a central bank or public authority or has a guarantee, is not necessarily linked to legally circulating currency and does not have the legal status of currency or money, but is accepted by individuals as a trading instrument or which may be transferred, stored or traded electronically and is not: (i) fiat currency, or (ii) electronic money, or (iii) financial instruments as defined in Part III of the First Appendix to the Services and Activities and Regulated Markets Law (L.87/2017), as this has been amended from time to time.

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

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

"Electronic money" has the meaning given to the term by Section 2 of the Electronic Money Law, excluding monetary value as referred to in paragraphs (a) and (b) of subsection (2) of Section 3 of the Electronic Money Law.

"Financial Institution" means:

a. an undertaking other than a credit institution, which carries out one or more of the activities listed in points (2) to (12), (14), and (15) of Annex IV of the Business of Credit Institutions Law, including the activities of currency exchange offices (bureaux de change)
b. an insurance or reinsurance undertaking within the meaning given to the term by Section 2 of the Insurance and Reinsurance Business and Other Related Issues Law, insofar as it carries out life assurance activities covered by the scope of the said Law
c. a firm or IF within the meaning given to the term by Section 2(1) of the Services and Activities and Regulated Markets Law (L.87/2017), as this has been amended from time to time
d. a collective undertaking marketing its units or shares
e. an insurance or reinsurance intermediary within the meaning given to the term by Section 356 of the Insurance and Reinsurance and Other Related Issues Law where it acts concerning life insurance and other related services
f. branches of any of the financial institutions as referred to in points (a) to (e), when they are in Cyprus, whether their head office is situated in a Member State or in a third country.

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

"High-Risk Third Country" means any third country according to the provisions of Paragraph (2) of Article 9 of the EU Directive through the adoption of delegated acts, which demonstrates strategic deficiencies in its national system for combating Money Laundering and Terrorist Financing, that pose significant threats to the financial system of the European Union, and a third country, classified by the Company as *high risk*, in accordance with the risk assessment provided for in Article 58A of the Law.

"Law" means the Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 to 2021, as amended from time to time.

"Manual" means the Company's AML/CFT & Procedures Manual (this manual).

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

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

"Money Laundering" means the money laundering offenses defined in Section 4 of the Law, referred to also the following:

a. Every person who (a) knows or (b) at the material time ought to have known that any kind of property constitutes proceeds from the commission of a *predicate offense* as this is defined in Section 5 of the Law, carries out the following activities:

   (i) converts or transfers or removes such property, to conceal or disguise its illicit origin or assisting in any way any person who is involved in the commission of the predicate offense to carry out any of the above actions or acts in any other way to evade the legal consequences of his actions
   (ii) conceals or disguises the true nature, the source, location, disposition, movement of, and rights concerning, property or ownership of this property,
   (iii) acquires, possesses, or uses such property
   (iv) participates in, associates, co-operates, conspires to commit, or attempts to commit and aids and abets and provides counseling or advice for the commission of any of the offenses referred to above
   (v) provides information concerning investigations that are carried out for laundering offenses to enable the person who acquired a benefit from the commission of a predicate offense to retain the proceeds or the control of the proceeds from the commission of the said offense
   (vi) commits an offense punishable by fourteen years' imprisonment or by a pecuniary penalty of up to EUR 500.000 or by both of these penalties in the case of (a) above and by five years' imprisonment or by a pecuniary penalty of up to EUR 50.000 or by both in the case of (b) above.

b. Further and for the purposes of point 1 above:

   (a) It does not matter whether or not the predicate offense is subject to the jurisdiction of the Cyprus Courts.
   (b) Laundering offenses may also be committed by perpetrators of predicate offenses.
   (c) The knowledge, intent or purpose required as elements of the offenses referred to above, may be inferred/concluded from objective factual circumstances.
   (d) No previous or simultaneous conviction for predicate offense from which the proceeds resulted is required.
   (e) It is not required to verify the identity of the person who has committed the predicate offense from whom the proceeds have originated.

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

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

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

"Politically Exposed Person (PEP)" means the natural person to whom or who has been entrusted with prominent public function in the Republic or in another country and his/her immediate family members and persons known to be close associates of such person

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

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

"Republic" means the Republic of Cyprus.

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

"Terrorist Financing" means the provision or gathering of funds by any means, directly or indirectly, to use such funds or knowing that they will be used in whole or in part for the commission of an offense within the meaning given to the term by Section 4 of the

International Convention for the Suppression of the Financing of Terrorism (Ratification and Other Provisions) Law and by Sections 5 to 13 of the Combating of Terrorism Law.

"Third Country" means a country that 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.

All other terms and definitions used in this Manual have the meaning provided by the Terms of Service. If any term or definition is not defined by this section of the Manual or by the mentioned Terms of Service, such a term or definition has the meaning provided by the applicable legislation.

2. INTRODUCTION

The purpose of the Manual is to lay down the Company's internal practices, measures, procedures, and controls relevant to the prevention of Money Laundering and Terrorist Financing, KYC (Know Your Client), and ATF (Anti-terrorist Financing).

The Manual is developed and periodically updated by the Money Laundering Compliance Officer (MLCO). In addition to the MLCO herself, the relevant duties of the MLCO are performed by the compliance department, which provides support to the MLCO. For the purposes of this Manual, the MLCO means both the MLCO herself and the employees of the compliance department who provide appropriate support. The Senior Management also provides MLCO with all necessary support.

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

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

The Manual has been prepared to comply with the provisions of the Law and the Combating of Terrorism and Victim Protection Law of 2019 (75(I)/2019), Regulation (EU) 2015/847 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 as well as other applicable laws and regulations.

3. THE RESPONSIBILITIES OF THE CEO

3.1. General

– Approve AML/CFT policy and allocate resources.
– Appoint the Money Laundering Compliance Officer (MLCO).

The responsibilities of the CEO concerning the prevention of Money Laundering and Terrorist Financing include the following:

a. to determine, record and approve the general policy principles of the Company in relation to the prevention of Money Laundering and Terrorist Financing and communicate them to the MLCO
b. to appoint the MLCO
c. to approve the Manual
d. to ensure that all relevant requirements of the Law and of the Directive are applied, and assure that appropriate, effective, and sufficient systems and controls are introduced for achieving the above mentioned requirement
e. to ensure that the MLCO, and his/her assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of Money Laundering and Terrorist Financing, have complete and timely access to all data and information concerning Clients' identity, transactions' documents (as and where applicable) and other relevant files and information maintained by the Company to be fully facilitated in the effective execution of their duties, as included herein
f. to ensure that all employees are aware of the person who has been assigned the duties of the MLCO, as well as his/her assistants (if any), to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing
g. to ensure that the MLCO and other responsible employees have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties
h. to implement adequate and appropriate systems and processes to detect, prevent and deter money laundering arising from serious tax offenses
i. to ensure that the Company's officials do not knowingly aid or abet Clients in committing tax offenses
j. approve the mandatory annual training program prepared by the MLCO,
k. ensure that it receives adequate management information on the implementation of the regulated entity's AML/CFT training program

l. to enhance further the AML/CFT measures adopted, when this is deemed necessary
m. ensure to be adequately trained to be well aware and up-to-date with the regulatory framework and the relevant responsibilities deriving from this.

4. MONEY LAUNDERING COMPLIANCE OFFICER

4.1. General

– Maintain and update this manual.
– Oversee client onboarding, transaction monitoring, and Suspicious Activity Reports (SAR).
– Liaise with the Financial Intelligence Unit (MOKAS) and other regulators.

In performing her role, the MLCO takes into account the nature, scale, and complexity of its business and the nature and range of services and activities undertaken in the course of that business.

4.2. Duties of the MLCO

During the execution of her duties and the control of the compliance of the Company with the Law and the Directive, the MLCO shall obtain and utilize data, information, and reports issued by international organizations, as these are stated in the Manual.

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

a. to design, based on the general policy principles of the Company mentioned above in point the Manual, the internal practice, measures, procedures, and controls relevant to the prevention of Money Laundering and Terrorist Financing, and describe and explicitly allocate the appropriateness and the limits of responsibility of each department that is involved in the abovementioned.
b. to review and update the Manual as may be required from time to time, and for such updates to be communicated to the CEO
c. to act as a first point of contact with the Unit, upon commencement of and during an investigation as a result of submitting a report to the Unit
d. to ensure the preparation and maintenance of the lists of Clients categorized following a *risk-based* approach, which contains, among others, the names of Clients, their account numbers, and the dates of the commencement of the Business Relationship. Moreover, the MLCO ensures the updating of the said list with all new or existing Clients, in light of any additional information obtained
e. to evaluate the systems and procedures applied by a third person on whom the Company may rely for Client identification and due diligence purposes, according to the Manual, and approve the cooperation with it
f. to identify and assess the sanctions risks to which the Company is exposed and implement a sanctions screening program in line with its nature, size, and complexity. Sanction screening is a control used to detect, prevent, and manage sanctions risk. Systems should be in place to detect newly designated sanctioned
individuals and to prevent the dissipation of assets
g. to implement a sanctions screening program created in line with the AML/CFT Program which should include:
(i) Policies: the requirements as to when screening needs to be done and at which frequency, how alerts should be handled and especially how to deal with the alerts if not enough information is available.
(ii) Responsible person: Potential sanctions matches should be reviewed by a person with appropriate skills and experience. The staff should be properly trained to know how to deal with potential sanctions matches.
(iii) Risk Assessment: Risk-based approach should be applied to decision-making regarding the set-up of sanctions screening program and this needs to be clearly documented.
(iv) Internal controls: It is necessary to document how the screening system is configured in order to demonstrate that it is reasonably expected to manage specific sanctions risks.
(v) During the execution of his duties and the control of the compliance of the Financial Organization with the Law and the present Directive, the compliance officer obtains and utilizes data, information, and reports issued by the relevant international organizations (i.e. FATF, MONEYVAL, CFSP, UN, IMOLIN, IMF).

5. RISK-BASED APPROACH

– Categorize clients by risk factors: HNWI/UHNWI status, PEP, jurisdiction, industry sector.
– Apply Enhanced Due Diligence (EDD) for high-risk categories.

The Company shall apply adequate and appropriate measures, policies, controls and procedures, depending on its nature and size, by adopting a risk-based approach, in order to mitigate and effectively manage the risks of Money Laundering and Terrorist Financing to focus its efforts on those areas where the risk of Money Laundering and Terrorist Financing appears to be comparatively higher.

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

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

Such measures include, *inter alia*:

a. identifying and assessing the Money Laundering and Terrorist Financing risks emanating from particular Clients or types of Clients, services, and geographical areas of operation of its Clients.
b. content moderation to detect and remove prohibited materials
c. automatic verification via the Sumsub system. The Sumsub service provider is to aid in the automated screening of Clients, to detect and assess whether the specific Client is subject to EU/UN and international sanctions (Clients are screened on more than 150 sanction lists), politically exposed person (PEP), convicted or suspected criminal
d. monitoring of Client transactions for suspicious activities based on triggers
e. system for assessing customer risk levels to monitor high-risk accounts
f. logging of Client actions and blocking of suspicious activity
g. managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures, and controls
h. continuously monitoring and improving the effective operation of the policies, procedures, and controls

The MLCO shall assess and evaluate the risks it faces, for usage of the services provided for the purpose of money laundering or terrorist financing.

5.1. Identification of Risks

The Company shall assess and evaluate the risk it faces, for usage of services provided for the purpose of money laundering or terrorist financing. The particular circumstances of the Company shall determine the suitable procedures and measures that need to be applied to counter and manage risk.

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

a. *Risks based on the Client's nature:*

- Complexity of ownership structure of legal persons
- Companies with bearer shares
- Companies incorporated in offshore centers
- PEPs
- Clients from *high-risk* countries or countries known for high levels of corruption or organized crime or drug trafficking
- The unwillingness of the Client to provide information on the Beneficial Owners of a legal person.
- Clients convicted for a Prescribed Offense (and already served their sentence)
- Clients with income and/or wealth from *high-risk* sectors such as arms, construction, gambling, and private military contractors.

b. *Risks based on the Client's behavior*:

- The unwillingness of Clients to provide information on the Beneficial Owners of a legal person.
- Frequent changes to Client due diligence information or payment details
- Client's origin of wealth and/or source of funds cannot be easily verified
- Are there adverse media reports or other relevant sources of information about the client, for example, are there any allegations of criminality or terrorism against the client or the beneficial owner?

c. *Geographical risk factors*:

- Countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems
- Countries identified by credible sources as having significant levels of corruption or other criminal activity
- Countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations
- Countries providing funding or support for terrorist activities or that have designated terrorist organizations operating within their country.

5.2. Relevant International Organizations

The Company, when assessing the money laundering and terrorist financing risks and when applying *risk-based* measures, should take into account, among others, the Risk Factor

Guidelines and the Guidelines issued by the Financial Action Task Force (the "FATF").

Further, on implementing appropriate measures and procedures on a *risk-based* approach, and on implementing the customer identification and due diligence procedures, the MLCO should consult data, information and reports (e.g. customers from countries that inadequately apply FATF, country assessment reports) that are published in following relevant organizations:

a. FATF
b. Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)
c. EU Common Foreign & Security Policy (CFSP)
d. UN Security Council Sanctions Committees
e. International Money Laundering Information Network (IMOLIN)
f. International Monetary Fund (IMF)
g. Joint Committee European Supervisory Authorities
h. Ministry of Foreign Affairs regarding the United Nations Security Council Resolutions or Decisions (Sanctions) or/and the European Union Council Decisions and Regulations (Restrictive Measures)
i. EU Sanctions Map

6. CLIENT ACCEPTANCE POLICY

– Conduct a preliminary risk assessment before onboarding.
– Reject or escalate any application lacking satisfactory documentation.

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

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

The General Principles of the CAP are the following:

a. the Company shall classify Clients into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Client
b. where the Client is a prospective Client, an account must be opened only after the relevant pre-account opening due diligence and identification measures and procedures have been conducted, according to the principles and procedures set in Section 11 of the Manual
c. all documents and data described in the Manual must be collected before and/or during accepting a new Client
d. no account shall be opened in anonymous or fictitious names(s).

6.3 Onboarding of High-Net-Worth Individuals (HNWI)
DMTECH CREDIT FUND LTD recognises that High-Net-Worth Individuals (HNWIs) may present a unique combination of elevated AML risk and strategic importance. As such, onboarding procedures for HNWIs are subject to enhanced scrutiny, in accordance with the firm's risk-based approach and applicable regulations.

6.3.1 Definition
A High-Net-Worth Individual (HNWI) is defined as a natural person who holds investable financial assets in excess of GBP 1,000,000 (or equivalent in another currency), excluding the value of their primary residence. This threshold may be adjusted in line with internal policy or regulatory guidance applicable in the jurisdiction of operation.

6.3.2 Enhanced Onboarding Procedures
Prior to establishing a business relationship with an HNWI, the following steps must be taken:

Completion of a detailed Source of Wealth (SoW) and Source of Funds (SoF) questionnaire;

Collection and verification of documentary evidence, which may include:

Certified bank statements;

Tax returns and wealth declarations;

Asset sale contracts or legal ownership certificates;

Auditor letters or independent confirmations (where appropriate);

Sanctions and PEP screening through approved third-party compliance providers;

Assignment of a risk score in line with DMT's AML Risk-Based Approach;

Mandatory review and sign-off by the Money Laundering Compliance Officer (MLCO) or their appointed deputy.

Where the HNWI is investing through a legal entity or trust, Ultimate Beneficial Ownership (UBO) and control structures must be fully documented and verified.

6.3.3 Data Protection and Confidentiality
Given the sensitivity of information involved, all HNWI onboarding records must be:

Stored in a segregated and encrypted environment, in compliance with UK GDPR and other applicable data protection laws;

Accessible only to authorised compliance and legal personnel;

Shared with third parties (e.g., KYC or legal service providers) only under strict confidentiality agreements and with documented justification.

6.3.4 Ongoing Monitoring and Review
Each HNWI relationship shall be subject to ongoing monitoring and reviewed at least annually. A review must also be triggered under the following circumstances:

A material change in the HNWI's financial profile or transaction behaviour;

A change of jurisdiction or control structure;

The appearance of risk indicators from internal systems or external sources.

All transactions must be monitored for consistency with the stated source of wealth, investment profile, and expected activity. Any deviation from expected patterns must be escalated to the MLCO.

7. CLIENT IDENTIFICATION AND DUE DILIGENCE PROCEDURES

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

- **Individuals (HNWI/UHNWI): Valid passport/ID, proof of address, source-of-fund declaration.**
- **Legal entities & structures: Certificate of incorporation, articles of association, ownership and control structure, powers of attorney.**

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

   a. when establishing a Business Relationship
   b. when carrying out Occasional Transaction that
      (i) amounts to EUR 15.000 or more, whether the transaction is carried out in a single operation or in several operations that appear to be linked
      (ii) constitutes a transfer of funds, as defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 exceeding EUR 1.000.
   c. when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction in the provision of the Services.
   d. when there are doubts about the veracity or adequacy of previous Client identification data.
   e. in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10,000 or more, whether the transaction is carried out in a single operation or in several operations that appear to be linked.

f. for Service Providers related to Crypto Assets, when carrying a transaction amounting to, or exceeding, one thousand euros (EUR 1,000), whether the transaction is carried out in a single operation or with several operations that appear to be linked.
g. when there is a suspicion of money laundering or terrorist financing, regardless of the amount of the transaction
h. when there are doubts about the veracity or adequacy of previously Client identification data.

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

a. The identification of the Client and the verification of the identity of the Client on the basis of documents, data or information issued or obtained from a reliable and independent source.
b. The identification of the beneficial owners' identity and taking reasonable steps to verify his/her identity to ensure that the Company is satisfied that it knows the beneficial owner. With regards to legal persons, trusts, companies, foundations and similar legal arrangements, reasonable steps should be taken to understand the structure of the ownership and Client control.
c. The assessment and, where appropriate, the collection of information on the purpose and the intended nature of the business relationship.

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

In this respect, it is the duty of the MLCO to apply all the relevant Client Due Diligence Identification Procedures described in the Manual for the cases mentioned above. Furthermore, the Head of the Support Department shall also be responsible for collecting and filing the relevant Client identification documents.

Further, the MLCO shall be responsible for maintaining at all times and using during the application of Client due diligence and identification procedures template-checklists with respect to required documents and data from potential Clients, as per the requirements of the Law and the Directive.

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

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

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

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

Monitoring is undertaken on an ongoing basis for customers and customers' related entities, directors, and beneficial owners.
Further to this the Company ensures:

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

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

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

The MLCO will:

- notify *Senior Management*,
- keep a clear, documented audit trail of the investigation of potential target matches and the decisions and actions taken, such as the rationale for deciding that a potential target match is a false positive.

7.2 Onboarding of High-Net-Worth Individuals (HNWI)
DMTECH CREDIT FUND LTD recognises that High-Net-Worth Individuals (HNWIs) may present a unique combination of elevated AML risk and strategic importance. As such, onboarding procedures for HNWIs are subject to enhanced scrutiny, in accordance with the firm's risk-based approach and applicable regulations.

7.2.1 Definition
A High-Net-Worth Individual (HNWI) is defined as a natural person who holds investable financial assets in excess of GBP 1,000,000 (or equivalent in another currency), excluding the value of their primary residence. This threshold may be adjusted in line with internal policy or regulatory guidance applicable in the jurisdiction of operation.

7.2.2 Enhanced Onboarding Procedures
Prior to establishing a business relationship with an HNWI, the following steps must be taken:

Completion of a detailed Source of Wealth (SoW) and Source of Funds (SoF) questionnaire;

Collection and verification of documentary evidence, which may include:

- Certified bank statements;
- Tax returns and wealth declarations;
- Asset sale contracts or legal ownership certificates;
- Auditor letters or independent confirmations (where appropriate);
- Sanctions and PEP screening through approved third-party compliance providers;
- Assignment of a risk score in line with DMT's AML Risk-Based Approach;
- Mandatory review and sign-off by the Money Laundering Compliance Officer (MLCO) or their appointed deputy.

Where the HNWI is investing through a legal entity or trust, Ultimate Beneficial Ownership (UBO) and control structures must be fully documented and verified.

7.2.3 Data Protection and Confidentiality
Given the sensitivity of information involved, all HNWI onboarding records must be:

Stored in a segregated and encrypted environment, in compliance with UK GDPR and other applicable data protection laws;

Accessible only to authorised compliance and legal personnel;

Shared with third parties (e.g., KYC or legal service providers) only under strict confidentiality agreements and with documented justification.

7.2.4 Ongoing Monitoring and Review
Each HNWI relationship shall be subject to ongoing monitoring and reviewed at least annually. A review must also be triggered under the following circumstances:

A material change in the HNWI's financial profile or transaction behaviour;

A change of jurisdiction or control structure;

The appearance of risk indicators from internal systems or external sources.

All transactions must be monitored for consistency with the stated source of wealth, investment profile, and expected activity. Any deviation from expected patterns must be escalated to the MLCO.

7.3. Transactions that Favour Anonymity

All verification steps run after initial identity checks via Sumsub:

- **Sumsub – Sanctions screening (EU/UN/OFAC), PEP lists, adverse media, biometric face-document matching.**

- **Cardamon (https://cardamon.ai) – AI agents extract applicable regulatory obligations, identify gaps in internal policies, and recommend immediate remediation steps.**

- **Vivox AI (https://www.vivox.ai / https://app.vivox.ai) – Advanced document authenticity checks and biometric verification using computer vision.**

- **Intrepid Fox (https://intrepidfox.ai) – Deep analysis of complex corporate and trust structures, uncovering hidden relationships and ultimate beneficial owners.**

Screening sequence: Sumsub → Cardamon → Vivox AI → Intrepid Fox

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

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

Perform full KYC when:

- **Establishing a new business relationship.**
- **Any single transaction ≥ €5,000.**
- **Suspicion arises in any transaction, regardless of amount.**
- **Client profile changes materially.**

Failure or refusal by a client to submit, before or during the establishment of a Business Relationship or the execution of an occasional transaction, the requisite data and information for the verification of his identity without adequate justification, constitutes elements that may lead to the creation of a suspicion that the Client is involved in money laundering or terrorist financing activities. In such an event, the Company shall not proceed with the establishment of the Business Relationship or the execution of the occasional transaction while at the same time, the MLCO considers whether it is justified under the circumstances to submit a report to the Unit.

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

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

7.5.1. General

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

a. the purpose of an account or relationship
b. the regularity or duration of the business relationship.

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

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

2. In case a liable entity enters into a new business relationship with a legal entity or with a trust or similar legal arrangement which is subject to the obligation to register information about its beneficial owner under the provisions of Sections 61A or 61B or 61C of the Law, the Company must collect proof of entry in the relevant register or an extract of the information on the beneficial owner from the relevant register.

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

4. Where the Company is unable to comply with the customer due diligence requirements laid down in paragraphs (a), (b) and (c) of subsection (1) of Section 61, it shall not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, according to the case, shall terminate the business relationship and examines the possibility submitting a suspicious transaction report to the Unit in relation to the customer, in accordance with the provisions of Section 69.

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

6. Under Section 61(2) of the Law, companies shall apply the Client identification procedures and Client due diligence measures referred to in Section 61 (1) of the Law but may determine the extent of such measures according to the degree of risk-taking into account at least the following variables (as per Annex I of the Law and as stated below):
    - the purpose of an account or relationship
    - the regularity or duration of the business relationship.

7. Under Section 61(3) of the Law for the purposes of the provisions on identification methods and customer due diligence measures, proof of identity is sufficient if:
    - It is reasonable to ensure that the Client is indeed the person who claims to be and
    - the person examining the evidence of the Client is satisfied, that the Client is in fact the person who claims to be.

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

9. Identification procedures and Client due diligence requirements shall be applied not only to all new Clients but also to existing Clients at appropriate times, depending on the level of risk of being involved in money laundering or terrorist financing (see points (b) to (d) of Section 11.1 of the Manual) including at times when the relevant circumstances of a Client change.

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

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

7.6.1. Natural persons residing in the Republic

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

    a. true name and/or names used as these are stated on the official identity card or passport
    b. e-mail address, if any
    c. date and place of birth
    d. nationality.

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

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

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

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

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

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

7.6.2. Natural persons not residing in the Republic

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

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

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

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

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

7.6.3. Accounts of legal persons

1. For Clients that are legal persons, the Company shall establish that the natural person appearing to act on their behalf, is appropriately authorized to do so and his identity is established and verified.

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

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

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

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

    a. certificate of incorporation
    b. certificate of good standing (up to 6 months), where available
    c. certificate of registered office
    d. certificate of directors and secretary
    e. certificate of registered shareholders in the case of private companies and public companies that are not listed in a Regulated Market of an EEA country or a third country with equivalent disclosure and transparency requirements
    f. memorandum and articles of association of the legal person
    g. a resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it
    h. in the cases where the registered shareholders act as nominees of the Beneficial Owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the Beneficial Owner, by which the registration of the shares in the nominee shareholder's name on behalf of the Beneficial Owner has been agreed

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

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

7. As an additional due diligence measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the Registrar of Companies and Official Receiver of the Republic (for domestic companies) or from a corresponding authority in the company's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as an operating company in the records of the Registrar of Companies and Official Receiver of the Republic or by an appropriate authority outside the Republic.

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

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

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

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

    a. the Company shall ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and Beneficial Owners.
    b. furthermore, the Company shall ascertain the nature of activities and the purpose of the establishment of the trust as well as the source and origin of funds by requesting the relevant extracts from the trust deed and any other relevant information from the trustees.

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

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

    a. The third person ***makes immediately available*** to the Company all evidence, data, information and identification documents which must be certified true copies of the originals or as otherwise acceptable by current business practices, that were

collected during the process of identification and Client due diligence, and forward directly to the Company copies of the documents and information on the identity of the Client and the beneficial owner where applicable.

b. The Company applies the appropriate due diligence measures on the third person with respect to his professional registration and procedures and measures applied from the third person for the prevention of Money Laundering and Terrorist Financing.
c. The ultimate responsibility for meeting those requirements of Client identification and due diligence shall remain with the Company and rely on the third person.

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

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

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

5. The Company shall ensure that the policies and procedures referred to in the above paragraph are effectively applied at the level of branches and subsidiaries majority-owned in the Member States and third countries as and if applicable.

6. The Company shall ensure that the third person gives its written approval for such cooperation which should be kept in the third person's file.

7. The Company shall keep a record of the information of the third party to which it relies for Client Identification and Due Diligence Purposes.

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

a. The Company relies on information provided by a third party which belongs to the same group
b. The said group applies Client due diligence measures, rules on record keeping and programs against money laundering and terrorist financing in accordance with the requirements of the EU Directive or equivalent rules

9. The Company may rely on third persons only at the outset of establishing a Business Relationship or the execution of an Occasional Transaction for the purpose of verifying the identity of their Clients.

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

a. make immediately available data, information and documents obtained as a result of the application of the procedures establishing identity and Clients due diligence measures
b. forward immediately to them, copies of these documents and relevant information on the identity of Client or the beneficial owner which the third party collected when applying the above procedures and measures.

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

7.8. Ways of Application of Client Identification and Due Diligence Procedures

Client identification procedures and Client due diligence measures shall comprise:

a. identifying the Client and verifying the Client's identity on the basis of documents, data or information obtained from a reliable and independent source
b. identifying the beneficial owner and taking risk-based and adequate measures to verify the identity on the basis of documents, data or information obtained from a reliable and independent source so that the person carrying on in financial or other business knows who the beneficial owner is, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the Client
c. assessing, and as appropriate, obtaining information on the purpose and intended nature of the business relationship
d. conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the person engaged in financial or other business in relation to the Client, the business and risk profile, including where necessary, the source of funds and ensuring that the documents, data or information held are kept up to date.
e. Screening Clients against databases or third-party checks for adverse tax-related news.

7.9. Transactions with regard to electronic money

The Company may not apply certain Client due diligence measures regarding transactions of electronic money if all the following mitigation factors are met:

a. the payment instrument is not reloadable or has a maximum monthly payment transactions limit of EUR 150 which can be used only within the Republic
b. the maximum amount stored electronically does not exceed EUR 150
c. the payment instrument is used exclusively for the purchase of goods or services
d. the payment instrument cannot be funded with anonymous electronic money
e. the issuer carries out sufficient monitoring of the transactions or business relationships to enable the detection of unusual or suspicious transactions.

The provisions above shall not be applied if cash withdrawals are made in cash and the amount involved exceeds one hundred euros (EUR 100).

The exception to the application of certain Client due diligence measures referred to in above does not include the obligation to conduct transaction and business relationship control on an ongoing basis as well as the obligation to trace and report suspicious transactions

7.10. Beneficiaries Information

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

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

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

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

The Company by the Legitimate Interest shall have access to

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

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

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

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

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

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

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

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

7.12. Ultimate Beneficial Owners ("UBOs") Central Registry

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

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

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

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

8. ON-GOING MONITORING PROCESS

8.1. 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:
   (i) 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
   (ii) transactions which, as of their nature, may be associated with money laundering or terrorist financing

8.2. Validity of KYC documentation

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

Two (2) months prior to the expiration of the KYC documentation, the Support Department is responsible for informing the Client and requesting a renewed valid KYC documentation. A reminder should be sent one (1) month prior to the expiration date. Records of the aforementioned notifications and reminders should be kept in the Company's records.

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

8.3.1. Full review and update

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

a. Clients: Yearly

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

9.2. Reporting of Suspicious Transactions to the Unit

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

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

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

9.3. Submission of Information to the Unit

The Company shall ensure that in the case of a suspicious transaction investigation by the Unit, the MLCO will be able to provide without delay the following information:

a. the identity of the account holders
b. the identity of the Beneficial Owners of the account
c. the identity of the persons authorized to manage the account
d. data of the volume of funds or level of transactions flowing through the account
e. connected accounts
f. about 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 authorization that have been given
    (vii) the type and identifying number of any account involved in the transaction.

9.4. Disclosure in Good Faith

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

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

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

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

The Law that provides for the Implementation of the Provisions of the United Nations Security Council Resolutions or Decisions (Sanctions) and the European Union Council's Decisions and Regulations (Restrictive Measures) is Law 58(I)/2016.

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

The Ministry of Foreign Affairs website (Theme 'Sanctions') lists relevant information regarding Sanctions/Restrictive Measures.

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

For EU restrictive measures:

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

For UN sanctions:

- General Information
- Consolidated List of Sanctions
- United Nations Security Council Resolutions
- United Nations Office on Drugs and Crime

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

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

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

The Company shall perform screening of its Clients against applicable financial sanctions target lists published in Cyprus Ministry of Exterior Consolidated Lists.

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

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

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

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

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

a. to consider the OFAC's Specially Designated Nationals List (SDN List) which is updated regularly, when assessing the money laundering (ML) and terrorist financing (TF) risks associated with business relationships and occasional transactions with its clients
b. to assess or reassess money laundering and terrorist financing risks, in the case of a business relationship with any person subject to Sanctions/Restrictive Measures.
c. in the case of a new/prospective customer who is subject to Sanctions/Restrictive Measures, to avoid the commencement of any business relationship with such a customer.

d. In the case of an existing customer who is subject to Sanctions/Restrictive Measures, to carefully examine the actions/measures that must be implemented (e.g. whether the freezing of funds/accounts is necessary, etc.) in accordance with the relevant UN Security Council Resolutions/Decisions and/or the EU Council's Decisions and Regulations.

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

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

11. RECORD-KEEPING PROCEDURES

11.1. General

The Support Department of the Company shall maintain records of:

a. Copies of documents and information that are necessary to comply with the Client due diligence requirements as defined in the Law and in this Manual including information obtained through electronic identification or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by a competent authority of the Republic,
b. The supporting evidence and records of transactions, consisting of the original documents or copies which are necessary to identify transactions,
c. The relevant correspondence documents with the Clients and other persons with whom a business relationship is maintained.

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

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

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

11.2. Format of Records

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

In case the Company will establish a documents/data retention policy, the MLCO shall ensure that the said policy shall take into consideration the requirements of the Law and as well as the applicable Data Protection Legislation.

It is also noted that in case the Company maintains transaction records that contain personal data of individuals, it shall take appropriate measures to protect the same as described under the applicable Data Protection Legislation.

11.3. Certification and language of documents

1. The documents/data obtained shall be in one of the following forms:
   a. original form or
   b. certified true copy form where certification is performed by the Company, in cases where the Company identifies the identity of the Client itself, after presented to the same in its original form, or
   c. certified true copy form where certification is performed by third parties, in cases where they verify the identity of the Client
   d. certified true copy form where the certification is performed by a competent authority or a person who, according to the relevant provisions of the laws of their country, is responsible for the authentication of documents or data. In that case, the documents should be certified copies (apostilled or notarized), or
   e. provided that at least one of the procedures referred to in Section this Manual is followed:
      - copy of the original or,

- data and information collected by electronic means of electronic verification.

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

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

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

   Provided that the Company assesses the results of the audit identity to meet the requirements of Section 61(3) of the Code Law. The Obligated Entity establishes mechanisms for the execution quality controls to evaluate the quality of information on which it intends to rely.

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

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

4. Use of Innovative Methods:

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

      (i) The use of such methods take place on a risk-based approach depending on the level of assets to be deposited and the size of transactions involved.
      (ii) A detailed assessment of the risks emanating from the use of such methods and of the measures employed to mitigate such risks has taken place in advance in accordance with of Part IV of the Directive, whereas such assessment is updated on an ongoing basis and it allows on a reasonable, consistent and demonstrable basis to conclude that the money laundering risks, including the risks of identity theft, impersonation and identity fraud, are sufficiently reduced.
      (iii) The Company must ensure that documentation, data and information gathered during the Client on-boarding process through innovative solutions remain accurate and up to date.
      (iv) The Company shall be responsible to set an explicit limit on the level of assets to be deposited and the size of transactions involved in order to be able to use an innovative identification method. Such limit is expected to vary per risk category and on a case-by-case basis, depending on the particular risks involved and on whether a combination of Innovative Client due diligence methods were used or were complemented with non innovative/non-electronic Client due diligence methods.
   b. Communicating with the Client through at an address that the Company has previously verified from an independent and reliable source, in the form of registered email e.g. direct mailing of account opening documentation, which the Client shall return to the Company or the sending of security codes required by the Client to access the accounts opened.

11.4. Data Protection, Record-Retention and Statistical Data

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

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

3. The right of access of the data subject to the data concerning him / her may be waived in part or in full according to the provisions of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018), as this has been amended from time to time:

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

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

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

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

12. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING

12.1. 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 anything that comes to their attention about transactions or any activity in a client's accounts for which there is a slight suspicion that is related to money laundering or terrorist financing according to the Law, the Company's employees shall fulfill their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after they comply with point (b) above.

12.2. Education and Training

12.2.1. Employees' Education and Training Policy

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

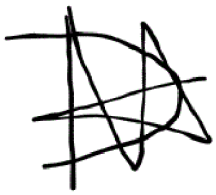
When setting up staff training, the MLCO shall consider:

a. which staff require training
b. what is the content of the training provided;
c. what form the training will take
d. how often training should take place
e. how staff will be kept up to date with emerging risk factors for the regulated entity.

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

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

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



APPENDIX 1

RISK FACTOR ASSESSMENT CHECKLIST

No.	Risks associated with a Client's and/or a Client's beneficial owner's business and/or or professional activity	YES	NO	COMMENTS / REMARKS
A1	Does the Client or beneficial owner have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defense, the extractive industries or public procurement?			
A2	Does the Client or beneficial owner have links to sectors that are associated with higher ML/TF risk, for example certain Money Service Businesses, casinos or dealers in precious metals?			
A3	Does the Client or beneficial owner have links to sectors that involve significant amounts of cash?			
A4	Where the Client is a legal person or a legal arrangement, does the company know what is the purpose of their establishment? For example, what is the nature of their business?			
A5	Does the Client have political connections, for example, are they a Politically Exposed Person (PEP), or is their beneficial owner a PEP?			
A6	Does the Client or beneficial owner have any other relevant links to a PEP? *(Where a Client or their beneficial owner is a PEP, the Company must always apply enhanced due diligence measures in line with Article 64 (1) (c) and (2) of the Law and Paragraph 9 of Fifth Appendix of the RAD 125/2020)*			
	• e.g. any of the Client's directors PEPs? If so, do these PEPs exercise significant control over the Client or beneficial owner?			
A7	Does the Client or beneficial owner hold another prominent position or enjoy a high public profile that might enable them to abuse this position for private gain? e.g.. are they senior local or regional public officials with the ability to influence the awarding of public contracts, decision-making members of high-profile sporting bodies or individuals who are known to influence the government and other senior decision makers?			

A8	Is the Client a legal person subject to enforceable disclosure requirements that ensure that reliable information about the Client's beneficial owner is publicly available, for example public companies listed on stock exchanges that make such disclosure a condition for listing?			
A9	Is the Client a credit or financial institution acting on its own account from a jurisdiction with an effective AML/CFT regime and is it supervised for compliance with local AML/CFT obligations?			
	• If so, is there evidence that the Client has been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years?			
A10	Is the Client a public administration or enterprise from a jurisdiction with low levels of corruption?			
A11	Is the Client's or the beneficial owner's background consistent with what the Company knows about their former, current or planned business activity, their business's turnover, the source of funds and the Client's or beneficial owner's source of wealth?			
No.	**Risks associated with a Client's or beneficial owners' reputation**	**YES**	**NO**	**COMMENTS / REMARKS**
B1	Are there adverse media reports or other relevant sources of information about the Client, for example are there any allegations of criminality or terrorism against the Client or the beneficial owner? If so are these reliable and credible? The Company should determine the credibility of allegations on the basis of the quality and independence of the source of the data and the persistence of reporting of these allegations, among other considerations. It should be noted that the absence of criminal convictions alone may not be sufficient to dismiss allegations of wrongdoing.			
B2	Has the Client, beneficial owner or anyone publicly known to be closely associated with them had their assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing?			

	● Does the Company have reasonable grounds to suspect that the Client or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?			
B3	Does the Company know if the Client or beneficial owner has been the subject of a suspicious transactions report in the past?			
B4	Does the Company have any in-house information about the Client's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship?			
No.	**Risk factors may be relevant when considering the risk associated with a Client's or beneficial owner's nature and behavior** ***(The Company notes that not all these risk factors will be apparent at the outset; they may emerge only once a business relationship has been established***	**YES**	**NO**	**COMMENTS / REMARKS**
C1	Does the Client have legitimate reasons for being unable to provide robust evidence of their identity, perhaps because they are an asylum seeker?			
C2	Does the Company have any doubts about the veracity or accuracy of the Client's or beneficial owner's identity?			
	● Does the Company have reasonable grounds to suspect that the Client or beneficial owner or anyone publicly known to be closely associated with them has, at some point in the past, been subject to such an asset freeze?			
C3	Are there indications that the Client might seek to avoid the establishment of a businessы relationship?			
C4	Is the Client's ownership and control structure transparent and does it make sense?			
	● if the Client's ownership and control structure is complex or opaque, is there an obvious commercial or lawful rationale?			
C5	Does the Client issue bearer shares or does it have nominee shareholders?			
C6	Is the Client a legal person or arrangement that could be used as an asset-holding vehicle?			

C7	Is there a sound reason for changes in the Client's ownership and control structure?			
C8	Does the Client request transactions that are complex, unusually or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale?			
	• Are there grounds to suspect that the Client is trying to evade specific thresholds such as those set out in Article 11(b) of Directive (EU) 2015/849 and national law where applicable?			
C9	Does the Client request unnecessary or unreasonable levels of secrecy?			
	• e.g. is the Client reluctant to share Client Due Diligence (CDD) information, or do they appear to want to disguise the true nature of their business?			
C10	Can the Client's or beneficial owner's source of wealth or source of funds be easily explained?			
	• e.g. through their occupation, inheritance or s? Is the explanation plausible?			
C11	Does the Client use the products and services they have taken out as expected when the business relationship was first established?			
C12	Is the Client a non-profit organization whose activities could be abused for terrorist financing purposes?			
No.	**Risk factors Company should consider when identifying the effectiveness of a jurisdiction's AML/CFT regime**	**YES**	**NO**	**COMMENTS / REMARKS**
D1	Has the country been identified by the Commission as having strategic deficiencies in its AML/CFT regime, in line with Article 9 of Directive (EU) 2015/849? (*Where the Company deals with natural or legal persons resident or established in third countries that the Commission has identified as presenting a high ML/TF risk, the Company must always apply EDD measures)*			

D2	Is there information from more than one credible and reliable source about the quality of the jurisdiction's AML/CFT controls, including information about the quality and effectiveness of regulatory enforcement and oversight?			
	• e.g. possible sources include mutual evaluation reports by the Financial Action Task Force (FATF) or FATF-style Regional Bodies (FSRBs) (a good starting point is the executive summary and key findings and the assessment of compliance with Recommendations 10, 26 and 27 and Immediate Outcomes 3 and 4), the FATF's list of high-risk and non-cooperative jurisdictions, International Monetary Fund (IMF) assessments and Financial Sector Assessment Program (FSAP) reports. It should be noted that membership of the FATF or an FSRB (e.g. MoneyVal) does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective.			
No.	**Risk factors Company should consider when identifying the effectiveness of a jurisdiction's AML/CFT regime**	**YES**	**NO**	**COMMENTS / REMARKS**
E1	Is there information, for example from law enforcement or credible and reliable open media sources, suggesting that a jurisdiction provides funding or support for terrorist activities or that groups committing terrorist offenses are known to be operating in the country or territory?			
E2	Is the jurisdiction subject to financial sanctions, embargoes or measures that are related to terrorism, financing of terrorism or proliferation issued by, for example, the United Nations or the European Union?			
	• e.g. the United Nations or the European Union?			
No.	**Risk factors Company should consider when identifying a jurisdiction's level of transparency and tax compliance**	**YES**	**NO**	**COMMENTS / REMARKS**
F1	Is there information from more than one credible and reliable source that the country has been deemed compliant with international tax transparency and information sharing standards?			
	• Is there evidence that relevant rules are effectively implemented in practice?			

	e.g. possible sources include reports by the Global Forum on Transparency and the Exchange of Information for Tax Purposes of the Organization for Economic Cooperation and Development (OECD), which rate jurisdictions for tax transparency and information sharing purposes; assessments of the jurisdiction's commitment to automatic exchange of information based on the Common Reporting Standard; assessments of compliance with FATF Recommendations 9, 24 and 25 and Immediate Outcomes 2 and 5 by the FATF or FSRBs; and IMF assessments (e.g. IMF staff assessments of offshore financial centers).			
F2	Has the jurisdiction committed to, and effectively implemented, the Common Reporting Standard on Automatic Exchange of Information, which the G20 adopted in 2014?			
F3	Has the jurisdiction put in place reliable and accessible beneficial ownership registers?			
No.	**Risk factors Company should consider when identifying the risk associated with the level of predicate offenses to money laundering**	**YES**	**NO**	**COMMENTS / REMARKS**
G1	Is there information from credible and reliable public sources about the level of predicate offenses to money laundering listed in Article 3(4) of Directive (EU) 2015/849?			
	• e.g. corruption, organized crime, tax crime and serious fraud? Examples include corruption perceptions indices; OECD country reports on the implementation of the OECD's anti-bribery convention; and the United Nations Office on Drugs and Crime World Drug Report.			
G2	Is there information from more than one credible and reliable source about the capacity of the jurisdiction's investigative and judicial system to effectively investigate and prosecute these offenses?			
No.	**Risk factors that may be relevant when considering the risk associated with a product, service or transaction's transparency**	**YES**	**NO**	**COMMENTS / REMARKS**

H1	To what extent do products or services allow the Client or beneficial owner or beneficiary structures to remain anonymous, or facilitate hiding their identity?			
H2	To what extent is it possible for a third party that is not part of the business relationship to give instructions, for example in the case of certain correspondent banking relationships?			
No.	**Risk factors that may be relevant when considering the risk associated with a product, service or transaction's complexity**	**YES**	**NO**	**COMMENTS / REMARKS**
I1	To what extent is the transaction complex and does it involve multiple parties or multiple jurisdictions, for example			
I2	To what extent do products or services allow payments from third parties or accept overpayments where this would not normally be expected?			
	• Where third party payments are expected, does the Company know the third party's identity, for example is it a state benefit or guarantor?			
	• Or are products and services funded exclusively by fund transfers from the Client's own account at another financial institution that is subject to AML/CFT standards and oversight that are comparable to those required under Directive (EU) 2015/849?			
I3	Does the Company understand the risks associated with its new or innovative product or service, in particular where this involves the use of new technologies or payment methods?			
No.	**Risk factors that may be relevant when considering the risk associated with a product, service or transaction's value or size**	**YES**	**NO**	**COMMENTS / REMARKS**
J1	To what extent are products or services cash intensive, as are many payment services but also certain current accounts?			
J2	To what extent do products or services facilitate or encourage high-value transactions?			

	● Are there any caps on transaction values or levels of premium that could limit the use of the product or service for ML/TF purposes?			
No.	**Risk associated with the way in which the Client obtains the products or services,**	**YES**	**NO**	**COMMENTS / REMARKS**
K1	Is the Client physically present for identification purposes?			
	● If not, has the Company used a reliable form of non-face-to-face CDD?			
	● Has it taken steps to prevent impersonation or identity fraud?			
K2	Has the Client been introduced by another part of the same financial group and, if so, to what extent can the Company rely on this introduction as reassurance that the Client will not expose the Company to excessive ML/TF risk?			
	● What has the Company done to satisfy itself that the group entity applies CDD measures to European Economic Area (EEA) standards in line with Article 28 of Directive (EU) 2015/849?			
K3	Has the Client been introduced by a third party, for example a bank that is not part of the same group, and is the third party a financial institution or is its main business activity unrelated to financial service provision?			
	● What has the Company done to satisfy itself that: i. the third party applies CDD measures and keeps records to EEA standards and that it is supervised for compliance with comparable AML/CFT obligations in line with Article 26 of Directive (EU) 2015/849;			
	ii. the third party will provide, immediately upon request, relevant copies of identification and verification data, inter alia in line with Article 27 of Directive (EU) 2015/849; and			
	iii. the quality of the third party's CDD measures is such that it can be relied upon?			

K4	Has the Client been introduced through a tied agent, that is, without direct Company contact?			
	• Can the Company be satisfied that the agent has obtained enough information so that the Company knows its Client and the level of risk associated with the business relationship?			
K5	If independent or tied agents are used, to what extent are they involved on an ongoing basis in the conduct of business?			
K5	Does the Company use intermediaries?			
	• If so, are the said intermediaries: i. regulated and subject to AML obligations that are consistent with those of Directive (EU) 2015/849?			
	ii. subject to effective AML supervision? Are there any indications that the intermediary's level of compliance with applicable AML legislation or regulation is inadequate, for example has the intermediary been sanctioned for breaches of AML/CFT obligations?			
	iii. based in a jurisdiction associated with higher ML/TF risk?