PAIRSTECH
CAPITAL MANAGEMENT LLP

PT 303 - ANTI MONEY LAUNDERING AND COUNTER TERRORIST FINANCING POLICY

February 2023

PAIRSTECH
CAPITAL MANAGEMENT LLP

Table of Contents

1. Document Control panel

1.1 Key Document Summary

Document Status	Complete
Document Owner	Emanuele Rigo
Approved By	Executive Committee
Date Approved	28/03/2022
Document Location	6 PT Compliance/Policies and Procedures
Next Review Date	8/02/2024

1.2 Document History

Date	Version	Status	Reviewers	Action/Comment
2/09/2019	01		Maria Mickiewicz	Designed to meet the Legal and Regulatory requirements of the United Kingdom and the 4th AML Directive on AML/CFT
22/09/2021	02		Emanuele Rigo	Update to meet the legal and regulatory requirements of the 6th AML Directive on AML/CFT
25/03/2022	03		Emanuele Rigo	Changes
15/06/2022	04		Executive Committee	Approval
08/02/2023	05	Current	Executive Committe	Changes on processes and update on lists and risk assessment

1.3 Scope of policy/document application

Entity: This Policy is relevant to the regulated entity Pairstech Capital Management LLP (the Firm). This Policy is also relevant to outsourcing any important or critical functions of THE FIRM.

Jurisdiction: THE FIRM is authorized and regulated by the FCA. This Policy is relevant to activity undertaken by THE FIRM in the UK and other jurisdictions, where the FIRM is authorized to provide its services.

Relevant Business Areas and Individuals: All employees permanent, contract and temporary and those under a contract for services with THE FIRM.

1.4 Connected documents

Countries list / Jurisdictions – AML Risk per Country List
Onboarding process
PT 308 - SANCTIONS COMPLIANCE POLICY

1.5 Review Periodicity

This policy shall be reviewed at least annually or at any time substantial changes to the relevant subject matter arise.

2. Introduction

The Company has been granted a license from the FCA as an Investment management Company. In this respect, it is under legal and regulatory obligation to design and implement a formal and effective AML/CFT Compliance and Sanctions Program. The Company's Board of Directors has nominated and appointed a MLRO/NO to design, implement, and manage this AML/CFT Compliance and Sanctions Program. The Company has designed several policies, including the AML/CFT Policy and other Compliance Policies, that must be strictly followed by all the members of staff of the Company.

Unlike previous AML regulations, which only prosecuted those individuals and organizations that directly profited from money laundering, the 6AMLD provides greater clarity on the type of crimes defined as money laundering or terrorist financing. For instance, criminal penalties are now the same for convicted individuals and those persons who aided and abetted them in money laundering or terrorist financing activities.

The onus is now on all regulated entities to take individual responsibility to ensure that their AML policies, procedures, and internal controls are adequate enough to detect and prevent money laundering and terrorist financing. The Company has low risk appetite toward and zero tolerance approach to AML CTF matters and it is committed to implementing and enforcing effective internal controls to counter risks deriving from such activities.

3. Regulatory and Legal Framework

This "Policy for preventing and combating money laundering and terrorism financing" (in brief: "AML policy") sets out to ensure that Pairstech Capital Management LLP (The "Company") complies with regulatory provisions on preventing and combating money laundering and terrorism financing, applying a risk-based approach, has an organizational structure, operational and control procedures, as well as IT systems suitable to guarantee compliance with the laws and regulations on anti-money laundering , taking into account the nature, size and complexity of the activities carried out, as well as the type and range of services provided.
The Policy applies to Pairstech ("Company"), its associates, or affiliates that provide investment management services to customers, as described in the applicable law(s), regulations, or directives of the respective country the entity is operating in, relating to the prevention of the use of the financial system for the purpose of money laundering and financing of terrorism. For the purposes of preventing and combating money laundering and financing of international terrorism, new regulations have been issued in recent years by the EU and Italian authorities.

3.1 Internationally

The Recommendations prepared by the International Financial Action Group (FATF) represent the fundamental standards for preventing and combating money laundering and terrorism financing are accompanied by "Interpretative Notes" which form an integral part of the new standards.

3.2 At EU Level

At the EU level, the main reference legislation consists of:

- EU Directive no. 2015/849 issued by the European Parliament and Council of 20 May 2015 on preventing use of the financial system for money laundering and terrorism financing, which modifies EU Regulation no. 648/2012 of the European Parliament and Council, repealing Directive 2005/60/EC of the European Parliament and Council and Directive 2006/70/EC issued by the European Commission (known as "IV Directive on anti-money laundering");
- EU regulation 2018/843 issued by issued by the European Parliament and Council of 30 May 2018, which modifies EU Regulation no. 2015/849 on preventing use of the financial system for money laundering and terrorism financing and which modifies Directive 2009/138/EC and 2013/36/EU ("V Directive on anti-money laundering");
- EU delegated regulation no. 2016/1675 issued by the European Commission on 14 July 2016 which supplements EU Directive no. 2015/849 of the European Parliament and Council, identifying high-risk third-party countries with strategic weaknesses;
- Joint guidelines issued on 26 June 2017 by the European Oversight Authorities (EBA, ESMA and EIOPA) regarding simplified and enhanced customer due diligence measures and risk factors.

3.3 In Italy

The main reference norm is represented by:
Legislative decree no. 231 of 21 November 2007, as last amended by legislative decree no. 90 of 25 May 2017, on "Implementing EU Directive 2015/849 on preventing use of the financial system for money laundering and terrorism financing, amending directives 2006/60/EC and 2006/70/EC and implementing EU regulation no. 2015/847 on information data accompanying transfers of funds, repealing EC Regulation no. 1781/2006 (hereinafter: legislative decree 231/2007);

- Legislative decree no. 109 of 22 June 2007 containing measures to prevent, oppose and repress terrorism financing and the activities of countries that threaten international peace and security, as latterly amended by the aforementioned legislative decree no. 90/2017.
- Legislative Decree 4 October 2019, no. 125 relating to amendments and additions to legislative decrees 25 May 2017, no. 90 and no. 92, implementing Directive (EU) 2015/849, as well as implementing Directive (EU) 2018/843 amending Directive (EU) 2015/849 relating to the prevention of using the financial system for money laundering or terrorism and amending directives 2009/138 / EC and 2013/36 / EU;
- Provision of Banca d'Italia on 26 March 2019 containing "Provisions regarding organization, procedures and internal controls aimed at preventing the use of intermediaries for money laundering and terrorism financing purposes" (hereinafter: "Organization and AML control provision");
- Banca d'Italia provision of 30 July 2019 containing provisions on customer due diligence to combat money laundering and terrorist financing;
- Banca d'Italia provision of 24 March 2020 containing provisions for the conservation of the making available of documents, data and information for the fight against money laundering and terrorism financing;
- Provision of the FIU, containing "Instructions on objective communications" of 29 March 2019;

3.4 In the UK

The main reference legislation consists of:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, amended by The Money Laundering and Terrorist Financing (Amendment) Regulations 2019;

4. Policy Applicability

This Policy applies to:

a. all senior managers, employees, officers, directors, appointed representatives, and contracted personnel of Pairstech, and to such other persons as designated by Pairstech from time to time (each an "Employee" or "member of staff" or "staff member" collectively "Employees", "members of staff" or "staff members"); and,
b. all natural and legal persons (and their respective employees, officers, and directors) that have contract relations with, perform services for or on behalf of Pairstech, including without limitation, clients, investors, suppliers, consultants, contractors, counterparties, and appointed representatives (each a "Customer" or "Associated Person," collectively "Customers" or "Associated Persons").

As a condition of doing business with Pairstech, Pairstech will require each Associated Person to accept that this Policy be incorporated into the contract entered into between the Associated Person and Pairstech.

Contracts and agreements executed between Pairstech, and Associated Persons may contain more specific provisions addressing some of the issues set out in this Policy. Nothing in this Policy is meant to supersede any more specific provision in a particular contract or agreement executed between Pairstech and an Associated Person, and to the extent, there is any inconsistency between this Policy and any other provision of a particular contract or agreement, the provision in the contract or agreement will prevail.

This Policy is intended to supplement and not replace other Pairstech codes of conduct, policies, rules, and procedures that are applicable to Senior Managers, Employees and Associated Persons from time to time. If any Employee or Associated Person has any doubt as to the codes, policies, rules, and procedures applicable in a given situation, or if any Employee or Associated Person perceives any conflict or inconsistency between this Policy and any other Pairstech code of conduct or any other Pairstech policies, rules, or procedures, then he/she should raise the issue with, and seek direction from the Pairstech Compliance Officer.

This Policy is a statement of principles and expectations for individual and business conduct. It is not intended to and does not in any way constitute a contract, an employment contract, or assurance of continued employment, and does not create any right in any Employee or Associated Person. The enforcement and interpretation of this Policy rests solely with Pairstech. This Policy only creates rights in favor of Pairstech. The headings contained in this Policy are for convenience only and shall not be interpreted to limit or otherwise affect the provisions of this Policy. In the event of any conflict between this Policy and applicable mandatory law, the applicable mandatory law shall prevail.

5. Purpose

The purpose of this policy is to:

a. Set out responsibilities of the Company and all parties it applies to as defined in Section 4., in respect of observing, complying and upholding policies on anti-money laundering ("AML") and counter-terrorist financiang ("CTF"); and

b. Provide information and guidance to Pairstech's members of staff on the risks pertaining AML, CTF and other financial crime, risks arising in relation to Pairstech's operations, due diligence procedures and how to assess and deal with issues, as they arises.
c. To comply with the provisions of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Money Laundering Regulations 2017), and the EU's most updated Money Laundering Directive (Directive EU 2018/1673);
d. To abide by the rules issued from time-to-time by the FCA and EU, and to assist the regulatory authorities in combating Money Laundering and Terrorist financing;
e. To abide by the FATF recommendations and Wolfsberg Group Guidance, especially those related to KYC and Remittances;
f. To ensure that company and its staff will not knowingly assist anyone to launder the proceeds of drugs sales, illegal businesses, embezzlement, terrorism or other acts prohibited as predicative offences in the United Kingdom;
g. To effectively meet all the requirements of "Know your Customer" process;
h. To comply with all the sanctions regimes and implement automated systems to check and validate if there is a direct or indirect connection to a sanctioned individual or entity;
i. To design and implement appropriate internal AML/CFT policies, procedures, and controls.

This Policy applies to all jurisdictions in which Pairstech operates.

6. Definitions

Term/Acronym Description
Account Manager is the person in charge of dealing with the Customer, Associate Person or other person as listed in Section 4, on an ongoing basis, as main point of contact between the firm and such persons.
AML – Anti-Money Laundering
BoD – Board of Directors or Executive Committee or management body as applies
Business relationship - any established business relationship having the company as a counterpart
CDD – Customer Due Diligence – it is the process of collecting, evidencing, and verifying the customer transactional behaviour.
CO – Compliance Officer
MLRO/NO – Money Laundering Reporting Officer/Nominated Officer;
Company – Pairstech Capital Management LLP, its associates, and or affiliates;
CFT – Combating the Finance of Terrorism;
EDD – Enhanced Due Diligence – it is the method of collecting additional evidences and answers about a customer during an investigation procedure.
FIU – Financial Investigation Unit;
KYC – Know Your Customer - it is the process that the financial services providers and other regulated entities must perform in order to identify their customers (existing or prospecting), collect and record relevant information, static and professional/business related data.
ML – Money Laundering – an act intended to have the effect of making any property a) that is, the proceeds obtained from the commission of an indictable offence under the laws of the United Kingdom, or b) that in whole or in part, directly or indirectly, represents such proceeds, not to appear to be or so represent such proceeds.
Money Laundering Risk – it refers to the risk of been engaged directly or indirectly with money laundering, terrorist financing, or proliferation.
Proliferation – It is the act of production, distribution, or usage of arms or armaments of mass destruction.

FCA – Financial Conduct Authority - the regulator of the financial services industry in the United Kingdom;
Risk-based approach – a reasonably designed risk-based approach is one by which institutions identify the criteria to measure the potential money laundering risks.
TF – Terrorist Financing – a) the provisions or collection, by any means, directly or indirectly, of any property (i) with the intention that the property be used, or (ii) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is actually so used); or b) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate; or c) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether, the person is a terrorist or terrorist associate.
UBO – Ultimate Beneficial Owner the natural person (or persons) that is the ultimate beneficiary when an institution initiates a transaction. The definition of who constitutes a UBO varies between jurisdiction, but generally a UBO is defined as an individual who holds a minimum of 10-25% (dependent on jurisdiction) of capital or voting rights in the underlying entity. For the purposes of this policy the Company shall identify all persons holding above 10% of capital.

7. Risk Assessment of Pairstech Activities

7.1 Overview

The Company has designed a Customer Risk Categorization methodology/model which has been incorporated in its AML System; based on this model, the customers are categorized into “High Risk”, “Medium Risk”, and “Low Risk” categories. The model is taking into consideration the following risk factors:

(a) Country Risk – it considers the country-related static data provided by the KYC details registered, i.e. “nationality”, “residency”, “ID issuing”, “beneficiary nationality”, “beneficiary residency”, “beneficiary bank’s residency”; it compares the risk based on the country categorization executed and published within the Sanctions Policy of the Company.
(b) Customer Risk – it considers the static data registered for the customer provided in the KYC procedure, i.e. the “profession” or “industry type”, the “identification document” if missing or expired, the type of residency (“resident”, “non-resident”, “tourist”, “diplomat” etc.).
(c) Money Laundering Risk – it considers any alerts generated for matching with sanctions or PEP public data.
(d) Product Risk – it considers the type of products that are used by the customer, i.e. derivatives, etc.

A broader description of the above mentioned risk factors can be found below.

7.1.1 Country Risk

The Company should consider whether the country of which the customer or other target of the KYC process is a citizen and/or resident is associated with high levels of organized crime, corruption, inadequate systems to prevent and detect ML/TF, and/or economic sanctions. If the country in question is determined to be higher risk in this regard, then the business relation must be escalated immediately to the CO and enhanced due diligence undertaken.

The Company has designed a Sanctions Policy, by which periodically identifies different sanctions and other data related to countries and territories; this data includes the Transparency International Index, the FATF high-risk and

NCCT list, different Regulators' specific instructions related to countries etc. After the identification of these risks and data, the Company categorizes the different countries to the following categories:

(a) low risk (Country List A)
(b) medium risk (Countri List B)
(c) high risk (Country List C)
(d) non-compliant or restricted (Country List R)

The Company periodically assesses the coherence of its Country List system against, but not limited the following databases:

1) Financial Action Task Force (FATF) List of High Risk and Monitored Jurisdictions (updated annually)[1]
2) Transparency International's Corruption Perceptions Index (updated annually)[2]
3) List of countries subject to economic sanctions by US[3], EU[4] and UK[5]
4) Basel AML Index[6]

7.1.2 Customer or Associated Person Risk

The Company serves a diversified customer portfolio, with individuals and corporates from different industries, profession types, residence types etc.; hence, the different risks associated with the "customer" are identified through our Customer Risk Categorization methodology/model and used in our Risk Scoring model in the AML System, as this is explained below. To this end, the Company considers the general criteria indicated by the reference legislation for assessing the risks of money laundering and terrorism financing associated with customers and for profiling them. In particular, it takes into account the following:

(a) HIGH RISK CUSTOMER:

(i) the type of subject (and/or its legal nature) and its characteristics;
(ii) the country or geographic area of origin (including funds), business relationships, the activity carried out and the countries with which there are significant connections, the economic and financial profile (in terms of income and assets);
(iii) uncooperative or reluctant behaviour in providing information;
(iv) negative reputational indices (e.g. criminal proceedings or for administrative liability, previous reports of suspicious transactions);
(v) structures that can be classified as asset interposition vehicles such as trusts, trust companies, foundations;
(vi) the inclusion in the lists of persons and entities associated with terrorism financing activities envisaged by EU Regulations or by the ministerial regulations adopted pursuant to legislative decree no. 109/2007;
(vii) type of economic activity (e.g. oil, health, construction, public procurement, defence, arms trade, extractive industry);
(viii) presence of a politically exposed person (PEP) or in any case holding a public office.

[1] https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)
[2] https://www.transparency.org/en/cpi/2021
[3] https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information
[4] https://sanctionsmap.eu/#/main
[5] https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases
[6] https://baselgovernance.org/basel-aml-index

(b) LOW RISK CUSTOMER:

(i) companies admitted to listing on a regulated market;
(ii) public administrations or bodies that perform public functions according to European Union law;
(iii) customers or beneficial owners resident in low-risk geographical areas;
(iv) EU banking and financial intermediaries or residents of a third country with an effective system to combat money laundering and terrorism financing (provided that the intermediary has not been subject to supervisory sanctions for non-compliance with anti-money laundering obligations).

7.1.3 Money Laundering Risks

The Company is using an AML System for the customer screening; therefore, there are alerts generated for watchlist and PEP matching of customers and based on these alerts we consider flagging the customers as "high risk" by default if there is any such alert confirmed. In this respect, the Customer Risk Categorization methodology/model and used in our Risk Scoring model in the AML System, as this is explained below.

7.1.4 Product and Activity Risks

Financial firms can be misused by money launderers or other criminal activities in a variety of ways, including via the exploitation of their services and structures. The firm must always understand and assess the circumstances in which any of its activities is conducted or its products are offered and decide whether or not the activity undertaken is at risk. Some examples of activities in which criminals may exploit the firm include (but are not limited to) the following:

(a) A customer submitting an application for investment service (portfolio management, advisory) can be considered as low risk for AML/CFT purposes;
(b) A customer submitting an application for investment service (execution only, corporate finance) is to be considered as medium risk;
(c) A customer applying for complex deal arrangement involving more than one counterpart is generally associated with medium to high risk;
(d) An introducer agreement with a third party is generally associated with medium risks;
(e) A portfolio management agreement can be assessed as low risk.

8. Policy notes

8.1 Know your customer (kyc) policy

The Customer Onboarding procedure is mandatory for all the relations and types of services involving members of Staff, Customers or Associated Persons as described into this policy.
The formal Customer Onboarding procedure is also mandatory for all the customers dealing in the name of and on behalf of a Corporate (legal entity), including the owners, managers, authorized persons, and beneficial owners. All the onboarded customers (physical and legal) must be identified and verified.

8.2 Customer acceptance policy

The Company has a customer acceptance policy and relevant procedures in implementation of the regulatory framework in force and of the best practices, so as to avoid relationship with customers against whom sanctions are applied or those who are facing charges for criminal activity, or those who may use Company services for ML, or TF, or other criminal activity.
The Company shall conduct due diligence of any person applying to do business with it. The staff shall obtain satisfactory evidence of the identity and legal existence of persons on the basis of reliable documents or other resources and record that identity and other relevant information regarding the customers in their files. If a customer refuses to provide his identity card or passport for verification, the relationship shall be refused. As per the customer acceptance policy of the Company and Risk Appetite Statement, the staff will follow the below guidelines:

(a) The Company deals with customers that have been formally identified at all times;
(b) The Company does NOT deal with non-profit organizations, except where these organizations have taken the written approval from the UK government;
(c) The Company does NOT deal with “shell banks”, “shell companies”, or “unidentified individuals”.

8.3 PEP client acceptance policy

Politically Exposed Persons are those who have been entrusted with prominent public function in a country or territory, or any of their family or closely related partners. The prominent public functions may in this regard include Heads of States, Heads of Government, Ministers, Dy. /Asst. Ministers, Senior Functionaries of Political parties, Members of Central Banks, Ambassadors, High Profile officers in Armed Forces, CEOs of State Undertakings and many more.

All business relationship with PEPs will be approved as these individuals are considered by default as high-risk customers, identified by the AML System and categorized by the automated Risk Categorization Model in the AML System, and are flagged as “PEP” in the onboarding software. Customer Registration will be established with all PEPs only after getting approval from the MLRO/NO. If any existing customer, or the beneficial owner of an existing corporate customer, has subsequently found to be linked to or has become PEP, then the relationship will be continued only after prior approval from the MLRO/NO.

PEPs are subject to EDD measures, and discreet inquiries must be made for ascertaining the purpose and ultimate beneficial owner.

8.4 Know your employee and employee training

As part of “Know Your Employee” program, the HR Department checks and verifies the collected documents presented during the recruitment procedure. The HR Department will collect all the appropriate educational qualification certificates, and or professional certificates, duly certified or attested by an appropriate authority. The HR Department will also execute a background check, or contact the referenced persons identified by the employee, so as to verify the correctness of the data and evidences provided. The HR Department also requests from the MLRO/NO to execute an independent background check for every employee from any sources that are available with the MLRO/NO, and any information found should be communicated confidentially to the HR Department with recommendations.

The Company offers AML/CTF training for all employees. The training is compulsory for new employees (part of the Induction Course) and is followed by a training on Basic Principles of AML/CFT and AML/CFT Policy and Procedures. Training is either provided by the Company internally, or through the Compliance Officer, or by other external firms engaged for this purpose. All the records related to training and employee undertaking are collected and stored. Furthermore, the Company has adopted a strategy to create a mandatory AML/CFT Refresher Course for every employee minimum once a year. Additional details can be found in Section 10.7.

9. DUE DILIGENCE PROCESS

The due diligence exercise is the process by which potential Customers and Associated Persons are screened to assess whether they present a material ML/TF risk. It involves identifying the person, verifying their identity, and undertaking high-level screening (i.e. financial, press and negative press, etc). The due diligence process also enables Pairstech to check that the Customer's profile is consistent with the purpose and objectives of the service Pairstech proveds.

The process should be risk-based, meaning that the higher the risk of ML/TF presented by the person, the more extensive the due diligence process should be. The risk-based approach ensures that disproportionate time is not spent reviewing low risk profiles.

The due diligence is therefore executed and based on the type of risks identified and the category of these risks; simple due diligence is exercised for low and medium risks, whereas enhanced due diligence is exercised for high risks.

Any member of staff liaising with Customers or any Associated Persons as defined into this policy must inform the Compliance department immediately at start of any discussion or business prospect and keep Compliance informed at any subsequent stage of establishing any form of business relationship. Such member of staff shall be considered an Account Manager as defined in this policy.

9.1 Customer Due Diligence

The CDD measures taken for every relationship are with persons listed in Section 4 comprises two steps: Identification and Verification.

(a) Identification is performed by gathering information from the person to the extent provided in Appendix A and Appendix B;
(b) Verification is performed by collecting supporting documentation to corroborate Identification process with copies of the original identification document, and/or via digital platform in use by the firm where such identity verification is required by circumstances (i.e. person is identified without the person being present).

Identification documents in a foreign language, other than English, should be translated by an authorized body and notarized by appropriate governmental bodies unless internal staff is able to provide adequate translation. In such latter case a translation shall be stored together with the original document and shall be deemed adequate only if such document is issued by countries in jurisdictions in Country List A.
Identification can be done also remotely via onboarding platform. In such case an independent evaluation and assent shall be given by the relevant member of staff.

9.2 Establishing the business relationship

Further to the identification process, we have to understand the nature of the business, profession, employment agreement, industry, etc the person is engaged in; and apply the appropriate risk scoring rating. The Customer Risk Categorization methodology/model will apply the risk score and category of each customer, thus considering the level of CDD applicable. The following table is deemed as non exhaustive.

Nature of activity	Jurisdiction	Risk	Type of Due Diligence
Application for investment service (portfolio management, advisory)	Country list A Country list B	Low Low	Standard Standard
Application for investment service (execution only, corporate finance)	Country list A Country list B	Medium High	Standard Enhanced
Application for complex deal arrangement	Country list A Country list B	Medium High	Standard Enhanced
Introducer agreement	Country list A Country list B	Medium High	Standard Enhanced
Portfolio management agreement	Country list A Country list B	Low Medium	Standard Standard

9.3 Maintenance of Customer Information

Since the type of business relationship that the Company has with its customers identified, the data and information of the customer and the beneficiary are continuously maintained. The account manager is the person in charge of dealing with the Customer, Associate Person or other person as listed in Section 4. Such information shall be stored appropriately following the Company's policy and standard. Such documentation shall be gathered through the onboarding software and there archived in digital format; if such documentation is obtained directly liaising with the person such documentation shall be digitalized and stored on the onboarding software and/or on the official Company cloud server.

Any further documentation, update or other relevant pieces of information shall be stored using the same system and, where possible in case it was not previously done, create an adequate record of the person.

9.4 Ultimate Beneficial Ownership

The Ultimate Beneficial Owners (UBOs) of a Corporate or an Incorporated Body are the individuals who hold singly and collectively a stake of 10% and above or controls the shareholding interest of more than 10%. All the UBOs must be identified, and proper CDD measures have to be taken, including the maintenance of the physical person's Customer Information as described above.

Ultimate Beneficial Ownership for complex corporate structure shall be determined with a thorough understanding of the such corporate structure and controlling chain. In such cases the relevant members of staff shall refer to Compliance Officer or MLRO to receive guidance.

Ultimate Beneficial Ownership shall be assessed in all cases unless it cannot be determined: in such cases reference shall be made to Compliance officer or MLRO to determine the case.

9.5 Non-Profit Organizations

It is the Policy of the Company NOT to deal with any Non-Profit Organizations, either local or international as they carry significant degree of ML/TF risk which cannot be mitigated by the Company and therefore is deemed inappropriate for the Risk Appetite of the firm.

9.6 Simplified customer due diligence

The Company applies Simplified Customer Due Diligence (SCDD) to the following types of customers provided the risk assessment performed does not ascertain higher risks:

(a) Financial Institutions, licensed by the FCA or other Regulatory Body in EU;
(b) Government, or semi-government body/department;
(c) Financial Institutions licensed in a reputable jurisdiction;
(d) Corporate that is listed in a reputable Stock Exchange.

The verification process as listed in Appendix A and Appendix B

9.7 Enhanced customer due diligence

The Company executes EDD on every customer belonging to the following categories:

(a) High Risk customers – when a customer has been categorized as a "high risk" by the Customer Risk Categorization methodology/model;
(b) Customers NOT physically present (no introducing meeting had a place) from Country List B (or higher risk);
(c) PEPs – in case a client is identified as a Politically Exposed Person;
(d) Client location/origin – high-risk jurisdictions or the list of countries in List C;

Enhanced due diligence (EDD) measures imply:

(a) the acquisition of more information relating to:
    (i) customer and beneficial owner (verification of ownership and control structure;
    (ii) evaluation of reputation information relating to proceedings or sanctions, activities carried out in the past and business or family ties found in the media or from reliable open sources);

(iii) ongoing relationship with specific regard to nature and purpose (analysis of the number, extent and frequency of operations to highlight possible inconsistencies;
(iv) reasons for which the customer requests a specific product when his needs could be met in another way or another country); - destination of funds (both the country and the purpose of use);
(v) the nature of the activity carried out.

(b) better quality of information:
(i) verification of the origin of the assets and funds used in the ongoing relationship (examination of financial statements, tax returns;
(ii) in case of high use of cash, verification of consistency with the activity carried out and turnover; in the case of operations with large banknotes, insights into the reasons behind this operation);

(c) higher frequency of updates:
(i) checks on the ongoing relationship to detect any changes in the customer's risk profile;
(ii) more frequent checks on operations to detect any elements of suspicion of money laundering (e.g. destination of funds and reasons for a given operation).

(d) authorization of the General Manager to start or continue the ongoing relationship.

In addition, to ensure constant monitoring of ML/TF risk, in the event of activation of the enhanced due diligence procedure, the Company provides for an authorization procedure which, in addition to the involvement of the hierarchical managers of the Business areas and the General Management, requires the intervention of the Anti-Money Laundering Unit in the presence of a particularly high-risk profile. The Company also pays particular attention to frequent cash transactions through careful monitoring and the determination of amount thresholds for payment and withdrawal transactions over a limited period of time, after which the opportunity to maintain the relationship must be assessed, raising the customer's risk profile. With reference to ongoing relationships or transactions with customers and beneficial owners who are politically exposed persons, except as indicated above, the Company has established that:

• PEPs are always attributed a high risk, as well as subjects related to them, even if not expressly considered by the reference legislation (e.g., delegates / delegates and coholders of continuous relationships);
• in order to check the status of PEP (both during the opening phase and during the monitoring phase of a relationship), in addition to the information provided by the customer, further sources such as official authority websites or commercial databases can be used by the Company or other information already collected in other locations (e.g. granting a credit line). The extension of the checks is commensurate with the degree of risk associated with the product or operation requested;
• The consent and maintenance of a relationship with a PEP is expressly approved by the General Manager, who assesses the exposure to the risk of money laundering of the PEP and the effectiveness of the risk mitigation measures adopted by the Company;
• in the event of a particularly high risk of money laundering, it is appropriate to continue to apply the adequate reinforced verification, even if the PEP has ceased to hold public office for over a year;
• enhanced due diligence measures involve the acquisition of the information necessary to establish the origin of the PEP assets and the funds used in the relationship or in the transaction. For this purpose, the customer's attestation must be verified on the basis of reliable documents from independent sources, provided by the customer himself or publicly available;
• the checks are intended to exclude that the funds used are the result of crimes of a corrupt nature or other criminal cases; these elements together with the customer's reluctance to provide information can be the subject of a suspicious transaction report;

• at least annually the AML unit, in the context of reporting to the Board of Directors, assesses the Company's exposure to the ML/TF risks associated with PEPs.

10. SYSTEMS AND CONTROLS

10. 1 Account Management

In order to comply with the latest regulations, the company shall assign to any business relationship an account manager nominated among its employees that will be the first point of contact with the customer or the business partner. Such individual shall, within the company, act as first point of contact and control toward the customer or business partner. Such individual shall, in accordance with the policies in place, work closely with compliance and the MLRO/NO to assess and monitor the business relationship.

10.2 Ongoing monitoring

The Company has set appropriate procedures in order to monitor the customer data, information; as a Policy the Company has set the following:
Keep the customer documentation and information updated: the Company reviews the data and maintains the required documents so as to make sure they are up-to-date. This shall include personal data, identification forms and business relationship;
Execute EDD: To execute EDD, the Company requires a valid evidence of Source of Funds (SoF);
Periodic checks: the company may determine to repeat, with periodicity adequate to the risks assessed, part of all of the due diligence of a customer or business partner;
Assess continuously the controls to be adequate: based on the business model it follows, the Company is considering the adequacy of controls imposed and adapts them in case there is anything identified;

10.3 Financial sanctions

In the Company's procedures, the automated scanning of names to identify possible matches with designated names is mandatory for all kinds of business relationship. The Company is using the publicly available sanctioned entity lists of UN Security Council OFAC SDN list, EU Consolidated Sanctions List, and UK-HMT Sanctions List. The company has an internal system to perform basic and enhanced checks and also uses external providers to confirm and verify information.
The company has adopted a Sanctions Policy to make sure to more promptly address all matters relating to the matter of sanctions.

10.4 Terrorist financing

The Company is abided by the UN Security Council Resolution 1373 (2001) whereby, and it takes every necessary step to prevent the financing of terrorism. The AML System is configured to download and maintain the UN lists related to the individuals and organizations that are subject to UN financial sanctions and is filtering all names to find if the customers or beneficiaries are related to terrorism. If there are any matches found, then a thorough investigation is executed so as to identify and verify properly these persons and prevent any business relationship with terrorists.

10.5 Tipping off

Tipping off is prohibited under the provisions of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Money Laundering Regulations 2017), that transposes the EU's Third Money Laundering Directive (2005/60/EC);
Since it is an offence based on the Law, the Company ensures that the management and employees are aware of and are sensitive to the data sharing, and consequences of tipping off;
In case the employee believes, or has reasonable grounds to believe, that a customer may be tipped off by conducting CDD measures or on-going monitoring, the employee should refer the case to MLRO/NO. The MLRO/NO shall maintain records to demonstrate the grounds for belief that conducting CDD measures or on-going monitoring would have tipped off the customer; and
Any letters, notices, or requests received from FCA, or FIU, or Police these should not be disclosed to any person outside the Compliance Team or customer.

10.6 Record keeping

The objective of record keeping is to ensure that we can provide necessary information about customers, and their details at any given time or as per the request of competent authorities, FCA, FIU, Law Enforcement Agencies, Courts, or Auditors/Examiners. All the receipts, records and documents are retained for a minimum period of five years after the end of the business relationship with the customer. These records can be stored as hard or soft copy, and strict process of document control is applicable. Strict confidentiality is maintained of all the customer's information, and related evidences. All members of staff are trained not to share any details related to customers.

10.7 Staff training

The Company is committed to the training and development of its members of staff, not only because it is mandatory by the Regulators, but because it is embedded in its business excellence model and values. All the members of staff of the Company are compulsorily trained on AML/CFT as follows:

(a) basic Principles of AML/CFT during the induction period, including the AML/CFT Policy and Procedures at inception;
(b) refresher AML/CFT Training to all members of staff, minimum once per year;
(c) advanced AML/CFT Training to all members of Senior Management once per year, so as to cover the different risk areas and risk assessment and reporting requirements; and
(d) all AML/CFT related Policies, Procedures, Forms, Templates, Work Instructions etc. are passed to every member of staff through an e-mail or is available on the Onedrive, they are obliged to read and keep updated with new developments and requirements.

11. Statutory Reporting

The MLRO/NO must ensure that the statutory reporting requirements under the AML or other Regulatory Requirements are strictly followed. The MLRO in conjunction with other Senior Managers shall ensure that a corporate culture of compliance with AML/CFT is established and upheld throughtout the organization.

12. Internal reporting

The MLRO/NO must prepare a complete and evidenced report to the Executive Committee at least every six months, detailing the different actions/activities executed during the reporting period and related to AML/CFT with the support of the designated account managers; the report is presented to the Executive Committee for discussion, and for acknowledgement of risks and mitigating measures.

The Executive Committee may give specific written instructions to the MLRO/NO for actions to be taken in order to comply fully with the Legal and Regulatory Framework described The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the Money Laundering Regulations 2017), and the EU's latest Money Laundering Directive (Directive EU 2018/1673).

The Company also authorises the MLRO/NO to give a brief weekly report to the CO, defining the different risk areas and activities the Compliance Function has executed; this report is copied also to the Management of the Company, and is considered as an overall guidance towards the appropriate AML/CFT risk mitigation procedures and controls.

13. Records

Pairstech should retain the original or a scanned copy/photocopy of documents used to identify and verify any of the target of the due diligence process, in addition to a record of other information (e.g. results of name screening) obtained in the course of completing the due diligence process outlined in this Policy. These records should be kept in relation to all persons who purport to act on their behalf, other connected parties, and/or any other organizations with whom Pairstech enters into a business relationship or any other relationship.

All documents and records mentioned in this policy and its Annexes should be kept throughout the relationship with the person and for a period of 5 years after the end of the relationship. Such records can be retained in paper or electronic form being the latter the preferred method.

14. APPENDIX A

1. Standard (Simplified) Due Diligence (Individuals)

The Company applies Simplified Due Diligence (SDD) to all individuals that require to be onboarded by the firm and that are not subject to Enhanced Due Diligence (as defined in this policy):

The identification as of the above is done by:

a. Identify: full name, place and date of birth, nationality, identity card number/travel document number, and proof of residential address.
b. Verify the information collected in (a) by
    i. viewing original color copy of the documents referenced below. If unable to view original copy, consider requesting copies of the documents in question which have been certified as "true copies" by a qualified solicitor, accountant, or other similar regulated professional.
    ii. by performing an ID Verification check via Fastdox facility which returns above 80% positive rate.

Individual	Documents required
Country list A	Identification Document (ID Card, Passport) [(1)] Proof of residential address from an official source (e.g., utility bill, bank statement, tax bill, official government correspondence, etc) – dated within the last three months.
All Other Country lists	Two forms of Identification Document (ID Card, Passport, driving license) [(1)] Proof of residential address from an official source (e.g., utility bill, bank statement, tax bill, official government correspondence, etc) – dated within the last three months.

No form of Identification can be fully guaranteed as genuine or representing correct identity. Account managers, sales representatives and other subjects working within the Company as identified as recipients of this policy in section [SECTION] should recognize that some types of documents are more easily forged than others. If suspicions are raised in relation to any document offered, Individuals should take whatever practical and proportionate steps that are available to establish whether the document offered is genuine or has been reported as lost or stolen. This may include searching publicly available information, approaching relevant authorities, or

requesting corroboratory evidence. Where suspicion cannot be eliminated, the document should not be accepted, and consideration should be given to making a report to the authorities.

2. Standard (Simplified) Due Diligence: Corporate and Institutional Entities

The Company applies Simplified Due Diligence (SDD) to all entities that require to be onboarded by the firm and that are not subject to Enhanced Due Diligence (as defined in this policy):

Financial Institutions, licensed by the FCA or other Regulatory Body in the UK or EU;
Government, or semi-government body/department;
Financial Institutions licensed in a reputable jurisdiction where a MOU is in place with the UK FCA;
Corporate entities that are listed in a reputable Stock Exchange;

a. Identify:
    i. Full legal name and trading name (if different);
    ii. Place and date of incorporation;
    iii. Corporate and business registration number;
    iv. Registered address and primary business address (if different);
    v. Nature/type of business;
    vi. Company's arrangements;
    vii. Regulatory body and register number;
    viii. Register of shareholders and controllers so to assess ultimate beneficial owners (UBOs); and
    ix. Register of directors or authorized signatories;
    x. Financial situation

b. Verification:
    i. The information gathered in 2(a) above should be verified to the extent possible using publicly available resources, including the Public Companies Registry (i.e. in the UK companies house) and ultimately requesting such documentation of the person target of the due diligence so to satisfy that all items listed under 2(a) are verified. Additional guidance is provided in Appendix B;
    ii. The verification procedures for individuals as set out in the first section of this Appendix A should be undertaken on individuals as in 2(a)viii and 2(a)ix.

Notes:
(1) The valid identification documents that can be accepted are:
National Identity Card: issued by a reputable government body, containing photograph for verification;
Travel Document/Passport: containing biodata and issued from a reputable government body;
National Driving License – issued by a reputable government body, containing photograph for verification.

15. APPENDIX B

Examples and guidance for several types of corporate bodies

The following guidance shall serve as a non exaustive list of documentation to be provided to the Company when a relation is started and it applies to any party involved with the firm including, but not limited to, members of staff, consultants, advisors, brokers, custodian banks, Introducers of business, any party that supplies services or goods to the Company.

1. NON-REGULATED PRIVATE COMPANY
    a. Certificate of Incorporation
    b. Memorandum and Articles of association (or equivalent)
    c. Register of Shareholders up to UBOs
    d. Register of Directors
    e. Authorised Signatory List (including signatory powers)
    f. Latest financial statement (if possible audited) or for newly incorporated companies an opening balance sheet signed by the Director

For individuals at 1(c), 1(d) and 1(e) follow guidance in Appendix A section 1.

2. REGULATED COMPANY
    a. Certificate of Incorporation
    b. Memorandum and Articles of association (or equivalent)
    c. Register of Shareholders up to UBOs
    d. Register of Directors
    e. Authorised Signatory List (including signatory powers)
    f. Latest financial statement (if possible audited) or for newly incorporated companies an opening balance sheet signed by the Director
    g. Proof of authorization from Regulator's public registry

For individuals at 2(c), 2(d) and 2(e) follow guidance in Appendix A section 1.

3. PARTNERSHIP
    a. Certificate of Incorporation
    b. Partnership Agreement
    c. Register of Members up to UBOs
    d. Authorized Signatory List (including signatory powers)
    h. Latest financial statement (if possible audited) or for newly incorporated companies an opening balance sheet signed by the Director.

For individuals at 3(c) and 3(d) follow guidance in Appendix A section 1.

4. FUND or other Collective Investment Scheme
    a. Certificate of Incorporation
    b. Offering memorandum, prospectus, supplements (master and or feeder fund, if applicable)
    c. Investment Management agreement
    d. For the Investment Manager please refer to Appendix B section 2
    e. Evidence of listing

f. Evidence of regulation (if applicable)
g. Register of Directors
h. Authorised Signatory List (including signatory powers)
i. Letter from Administrator or AIFM advising on onboarding process of subscribers in relation to CDD and AML policy.

For individuals at 4(g) and 4(h) follow guidance in Appendix A section 1.

5. TRUST/FOUNDATION

a. Trust deed and sub-trust deed
b. Evidence of Trustees
c. Evidence of Settlors
d. Authorized signatory list (including signatory powers)
e. Evidence of Beneficiaries
i. Latest financial statement (if possible audited) or for newly incorporated companies an opening balance sheet signed by the Director.

For individuals at 5(b), 5(c, 5(d) and 5(e) follow guidance in Appendix A section 1.

6. OTHER COMPLEX STRUCTURES

For other structures where more than a layer of control is involved the account manager or sales representative shall assess the control chain up to the ultimate beneficial owners. On such complex structures the Company mandates that the client-facing members of staff do contact compliance department to assess the nature and scope of due diligence process to apply.

16. APPENDIX C

AML – Risk per Country Lists

LIST A - LOW RISK	LIST B - MEDIUM RISK	LIST C - HIGH RISK	RESTRICTED/SANCTIONED
EUROPE	**EUROPE**	**EUROPE**	
LATVIA	CROATIA	RUSSIA	VENEZUELA
PORTUGAL	MALTA	TURKEY	LYBIA
UK	HUNGARY	NORTH MACEDONIA	TURKMENISTAN
FRANCE	BULGARIA	UKRAINE	SOMALIA
DENMARK	SERBIA	ARMENIA	SOUTH SUDAN
FINLAND	UZBEKISTAN		BELARUS
ANDORRA	TAJIKISTAN		NORTH KOREA
SWEDEN	KYRGYZSTAN		IRAN
ICELAND	GEORGIA		
SLOVENIA	MOLDOVA		
ITALY	ALBANIA		
LITHUANIA	AZERBAJAN		
NORWAY	ISOLA DI MAN		
GREECE			
SPAIN			
CZECH REPUBLIC			
IRELAND			
BELGIUM			
AUSTRIA			
NETHERLANDS			
GERMANY			
SLOVAKYA			
POLAND			
SWITZERLAND			
CYPRUS			
LIECHTENSTEIN			
SAN MARINO			
NORTH AMERICA	**NORTH AMERICA**	**NORTH AMERICA**	
CANADA	GUERNSEY		
UNITED STATES OF AMERICA			
EAST ASIA AND PACIFIC	**EAST ASIA AND PACIFIC**	**EAST ASIA AND PACIFIC**	
AUSTRALIA	SOLOMON ISLANDS	HONG KONG	
JAPAN	PHILIPPINES	TONGA	
NEW ZELAND	INDONESIA	VIETNAM	

SOUTH KOREA	MONGOLIA	CAMBODIA	
SINGAPORE	MACAO	MYANMAR	
TAIWAN	CHINA	VANUATU	
		FIJI	
		GUAM	
		PALAU	
		SAMOA	
		MALAYSIA	
		THAILAND	
		SAMOA USA	
SOUTH ASIA	SOUTH ASIA	SOUTH ASIA	
	BANGLADESH		
	SRI LANKA		
	BHUTAN		
	PAKISTAN		
LATIN AMERICA	LATIN AMERICA	LATIN AMERICA	
CHILE	GRENADA	JAMAICA	
ARGENTINA	PERU	HAITI	
	COLOMBIA	PANAMA	
	SAN KITTS AND NEVIS	TRINIDAD E TOBAGO	
	CUBA	BAHAMAS	
	ANTIGUA E BARBUDA	BARBADOS	
	ARUBA	COSTA RICA	
	NICARAGUA	DOMINICAN REPUBLIC	
	GUATEMALA	URUGUAY	
	HONDURAS	VIRGIN ISLANDS	
	SAINT LUCIA	TURKS AND CAICOS ISLANDS	
	ANGUILLA	JAMAICA	
	ARUBA		
	BELIZE		
	BERMUDA		
	CAYMAN		
	CURACAO		
	MEXICO		
MIDDLE EAST AND NORTH AFRICA	MIDDLE EAST AND NORTH AFRICA	MIDDLE EAST AND NORTH AFRICA	
	BAHRAIN	ISRAEL	
	EGYPT	JORDAN	
	TUNISIA	QATAR	
	SAUDI ARABIA		

	MOROCCO		
	UNITED ARAB EMIRATES		
	OMAN		
SUB SAHARAN AFRICA	SUB SAHARAN AFRICA	SUB SAHARAN AFRICA	
	MAURITIUS	NIGER	
	ZIMBAWE	BENIN	
	BURKINA FASO	UGANDA	
	MALAWI	CAMEROON	
	GHANA	MAURITIANA	
	SUD AFRICA	ESWATINI	
	ZAMBIA	SIERRA LEONE	
	CAPE VERDE	SENEGAL	
	TANZANIA	MALI	
	NIGERIA	GUINEA BISSAU	
	ETIOPIA	MADAGASCAR	
	KENYA	MOZAMBICO	
		CONGO	
		BOTSWANA	
		SEYCHELLES	