Approved by
the Resolution dated 18.02.2025 of the
Sole Shareholder of O P E S Commercial Brokers L.L.C

OPES Commercial Brokers L.L.C

Anti-Money Laundering Policy

Dubai, 2025

Table of Contents

1. General

This Anti-Money Laundering Policy (the " AML Policy") of OPES Commercial Brokers L.L.C. (the "Firm") was developed in accordance with the regulatory legal acts of the UAE, namely the Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations, international conventions and treaties ratified by the UAE.

All members of senior management and employees, including full-time and part-time employees, contractors, and interns at OPES Commercial Brokers L.L.C must be familiar with this Policy and pay attention to the suspicious activities of the client and promptly notify MLRO.

This Policy aims to prevent the Firm and its employees from involvement in money laundering and terrorist financing ("ML/TF"), while safeguarding the OPES Commercial Brokers L.L.C reputation.

Nature of money laundering. The term "money laundering" covers a wide range of activities and processes intended to alter the identity of the source of illegally obtained money in a manner which creates the appearance that it has originated from a legitimate source. In this Policy, a reference to 'money laundering' also includes a reference to terrorist financing.

Nature of terrorist financing. The term "terrorist financing" includes making available funds or financial services, 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. Terrorist or terrorist organizations require financial support to achieve their aims. There is often a need for them to obscure or disguise links between them and their funding sources. It follows then that terrorist groups must similarly find ways to launder funds, regardless of whether the funds are from a legitimate or illegitimate source, to be able to use them without attracting the attention of the authorities.

The Firm, primarily engaged in providing legal services, might be likely to be used during the all stages of money laundering: placement, layering, and integration. This risk arises from activities such as handling client funds, forming legal entities or trusts, and providing legal advice. Criminals may exploit these services to introduce illicit funds into the system, obscure asset ownership, or facilitate the transfer of illegal funds through legal arrangements. The Firm acknowledges these risks and implements appropriate measures to detect and prevent the misuse of its services for ML/TF.

2. Definitions

Terms used in this Policy have the same meanings as they have, from time to time, in the Acting Law of the UAE, unless the contrary intention appears.

- **AML Lists** – Sanctions list, and internal monitoring list, PEPs list as defined below. The AML list includes the following lists:

- **Sanctions list** - a list of individuals and legal entities associated with ML/TF and financing the proliferation of weapons of mass destruction on an international and national scale. It includes:
    - *AFM Lists* – a list of persons involved in terrorist activities, a list of organizations associated with the financing of terrorism and extremism compiled in accordance with the requirements of the AML Regulations, as well as a list of organizations and persons associated with financing the proliferation of weapons of mass destruction made in accordance with the requirements of the AML Regulations and posted on the AFM web-resources.
    - Consolidated United Nations Security Council Sanctions List.
    - UN sanctions and resolutions.
    - Specially Designated Nationals and Blocked Persons List (SDN List) administered by the Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury.
    - European Union Consolidated Financial Sanctions List.
    - UK Consolidated Financial Sanctions List (HMT list) maintained by HM Treasury – entities and individuals subjected to certain financial restrictions as part of the United Kingdom's government's domestic counter-terrorism regime policy.
- **Internal Monitoring List** – a list of individuals and legal entities with a high risk of ML/TF. The Internal Monitoring List includes the following lists and lists:
    - *List under MLRO's control* – list of the Firm's customers, for which the MLRO exercises special control and monitoring, due to the MLRO's suspicions that the client's activities are related to ML/TF.
- **PEPs List**:
    - The list of public officials is approved by the Cabinet Decision of UAE.
    - Lists of public officials of the international online databases or publicly available sources for monitoring individuals for risks, negative and other information, to combat money laundering, combat corruption and bribery, economic and other sanctions.

- **AML Regulations** – the list of legal acts the Firm is required to adhere:
    - Federal Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations (as amended by Federal Decree Law No. (26) of 2021),
    - Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulationof Decree-Law No. (20) of 2018 On Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (as amended by Cabinet Resolution No. (24) of 2022).
    - Apart from the above, one needs to adhere to the following legislation:
    - The Cabinet Decision No. (109) of 2023 On Regulating the Beneficial OwnerProcedures
    - Cabinet Resolution No. (132) of 2023Concerning the Administrative Penalties against Violators of The Provisions of the Cabinet Resolution No. (109) of 2023 Concerning the Regulation of Beneficial Owner Procedures
    - Cabinet Decision No. (16) of 2021 Regarding the Unified List of the Violations and Administrative Fines for the Said Violations of Measures to

Combat Money Laundering and Terrorism Financing that are Subject to the Supervision of the Ministry of Justice and the Ministry of Economy,

- Cabinet Resolution No. (74) of 2020 regarding the Terrorism Lists Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combatting of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing, and Relevant Resolutions.

- **Beneficial owner**, (1) in relation to a customer, is: (a) for an account – a natural person who ultimately owns, or exercises effective control over the account; (b) for a transaction – a natural person on whose behalf or for whose benefit the transaction is being conducted; (c) for a legal person or arrangement – a natural person who ultimately owns or exercises effective control over the legal person or arrangement. (2) Without limiting (1) (c), the beneficial owner for: (a) a legal person includes: (i) a natural person who, *directly or indirectly, owns or controls at least 25% of the shares*, participation interest or voting rights of the legal person; or (ii) a natural person who, *directly or indirectly, otherwise exercises control over the legal person's management*; (b) a legal arrangement that administers and distributes funds (such as a trust) includes: (i) where the beneficiaries and their distributions have already been determined - a natural person who is to receive at least 25% of the funds of the arrangement; (ii) where the beneficiaries or their distributions have not already been determined – a natural person who is part of the class of natural persons for whose benefit the arrangement is established or operated and who could receive at least 25% of the funds of the arrangement; or (iii) where a natural person, directly or indirectly, exercises control over at least 25% (by value) of the property of the arrangement.
- **Customer/Client** - An individual or legal entity becomes a client (customer) when a business relationship is formalised by signing Firm's services agreement.
- **Employees** - all members of senior management and employees, including full-time and part-time employees, contractors, and interns at OPES Commercial Brokers L.L.C .
- **Financial Action Task Force (FATF)** - an intergovernmental organization for developing and implementing international standards to combat money laundering and terrorist financing.
- **Foreign entity without legal personality** - refers to a fund, partnership, trust, company, association, or any other corporate entity formed in accordance with the legislation of a foreign country. These structures are considered distinct organizational and legal forms, regardless of whether they have the status of a legal entity in the foreign country where they are established. All foreign legal entity customers of the Firm shall be treated as foreign entity without legal personality under the definition of AML Regulations.
- **Relevant Authorities (AFM)** - state bodies of the UAE, which performs financial monitoring and takes measures on AML/CFT.
- **Politically Exposed Person (PEP).** A PEP is a natural person (including a family member or known associate) who is or has been entrusted with a prominent public function, including but not limited to: a head of state or of government, senior politician, member of a legislative or constitutional assembly, senior government official, senior judicial official, senior military officer, ambassador, senior person in an international organization, senior executive of a state-owned entity, a senior political party official, or an individual who has been entrusted with similar functions such as a director or a deputy director; at an international, national, or regional

level. This definition does not include middle-ranking or more junior individuals in the above categories.

- *Foreign PEPs:* individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- *Domestic PEPs:* individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- *International organization PEPs:* persons who are or have been entrusted with a prominent function by an international organization, refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e. directors, deputy directors and members of the board or equivalent functions.
- *Family members* are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership.
- *Close associates* are individuals who are closely connected to a PEP, either socially or professionally.

- **Senior Management –** in relation to the Firm: every member of the Firm's executive management, including but not limited to the Senior Executive Officer ("SEO"); in relation to a **Customer** that is a Body Corporate: every member of the Body Corporate's Governing Body and the person or persons who control the day-to-day operations of the Body Corporate, including its Senior Executive Officer, Chief Operating Officer and Chief Financial Officer.

3. MLRO function and Internal Control Requirements

3.1. Responsibility for the Firm's compliance with this Policy lies with the every member of its Senior Management, including but not limited to the Firm's SEO. Senior Management must be fully engaged in the decision-making processes and must take ownership of the Risk-Based Approach (RBA).

3.2. The Senior Management of the Firm is responsible for implementing effective AML systems and controls that can adequately manage the ML/TF risks identified.

3.3. In order for the MLRO to discharge responsibilities effectively, Senior Management should, as far as practicable, ensure that the MLRO is:

a) appropriately qualified with sufficient AML knowledge;

b) subject to the constraint of the Firm's size, independent of all operational and business functions;

c) resident in the Dubai;

d) of a sufficient level of seniority and authority within the Firm;

e) provided with regular contact with, and when required, direct access to Senior Management to ensure that Senior Management is able to satisfy itself that statutory obligations are being met and that the business is taking sufficiently effective measures to protect itself against ML/TF risks;

f) fully conversant with the Firm's statutory and regulatory requirements and the ML/TF risks arising from its business;

g) capable of accessing, on a timely basis, all available information (both from internal sources such as CDD records and external sources such as circulars from the relevant authorities; and

h) equipped with sufficient resources, including staff and appropriate cover for the MLRO's absence (i.e., an alternate or deputy MLRO who should, where practicable, have the same status).

3.4. The Money Laundering Reporting Officer (MLRO), appointed by the resolution of the Shareholder(s) of the Firm oversees and coordinates the Firm's AML initiatives. A Deputy MLRO assumes these duties in the MLRO's absence.

3.5. The MLRO must meet the following requirements:

a) Higher education in law, finance, or a related field;

b) At least two years of AML-related work experience;

c) An impeccable business reputation.

3.6. The responsibilities and functions of the MLRO under this Policy include, but are not limited to, the following:

i) Ensuring that the Firm has in place internal AML policy and procedures approved by the Senior Management and monitoring their effective implementation.

j) Carrying out MLRO responsibilities in accordance with the AML Regulations.

k) Overseeing the accurate and timely submission of reports to the AFM and notifications to the Relevant Authorities' AML Department as required under AML Regulations.

l) Determining whether client activities are suspicious and, if so, reporting to the AFM and notifying the Relevant Authorities, following internal procedures.

m) Preparing reports for Senior Management outlining the results of AML controls and proposing enhancements to AML risk management and internal controls.

n) Requesting Senior Management decisions on establishing, maintaining, or terminating client relationships in accordance with the AML Regulations and the Firm's AML Policy.

o) Informing the Senior Management about AML violations, staff non-compliance, and disciplinary actions taken.

p) Acting as the primary contact for the relevant authorities, receiving and timely submitting STRs/TTRs and responding to requests for information.

q) Maintaining a register of all reports submitted to regulatory authorities.

r) Ensuring proper retention of CDD documents, STR records, and communications with authorities.

s) Delivering regular AML training to Firm employees in line with AML Regulations.

t) Safeguarding the confidentiality of all information obtained while performing AML duties.

u) Ensuring secure storage and management of documents and files received from the Firm's employees for the required period by AML Regulations.

3.7. To effectively fulfill their assigned functions, the MLRO is granted the following powers:

a) Issue recommendations and binding instructions to Employees on establishing, continuing, or terminating business relationships with clients, in accordance with the Firm's AML Policy.

b) Access all Firm premises, information systems, telecommunications facilities, documents, and files necessary for carrying out AML functions, as stipulated in internal procedures.

c) Conduct AML-focused audits of structural subdivisions and provide recommendations to eliminate identified deficiencies or violations.

d) Organize and lead meetings to discuss matters related to the internal AML control framework.

e) Engage personnel from other structural divisions in developing and implementing AML-related internal control measures.

f) Collaborate with structural divisions, employees, Senior Management, and the Shareholder(s) in exercising internal AML controls.

3.8. The Senior Management must provide full support to the MLRO in AML matters as outlined in this AML Policy. Responses to any AML-related requests from the MLRO must be timely and thorough. Employees who interact with clients are specifically required to report any unusual or suspicious behavior exhibited by clients without delay. Any employee who has knowledge of, suspects, or has reasonable grounds to suspect money laundering or terrorist financing must report the matter to the MLRO in writing, either by email or by submitting relevant documentation in hard copy. Reports should include relevant details, such as information about the parties involved, and reasons for suspicion.

3.9. Should an Employee become aware of AML regulation breaches committed by colleagues or Senior Management, they are obligated to immediately inform the MLRO. MLRO shall confirm the receipt of such information within ten business days and conduct an internal investigation within two months of receiving such request and take appropriate measures within the bounds of the law and Firm's policies. In some cases, the MLRO might involve the Senior Executive Officer as deemed necessary, considering there

is no conflict of interest. In the event the MLRO is implicated in such a violation, Employees must report to both the SEO and Shareholder(s). If requested, Employees must fully cooperate with law enforcement agencies, regulatory bodies, and other authorities investigating money laundering or related criminal activities.

3.10. As part of implementation of the AML Policy, the following computer-based data systems are used by the Firm for AML compliance:

a) Web-SFM to submit Suspicious Transaction Reports (STRs) and other required notifications to the Relevant Authorities in accordance with AML Regulations.

b) Secured platforms for storing client data. All client identification, verification, and other data are stored on secure servers managed by the Firm. Access is restricted to authorized personnel and monitored to prevent unauthorized disclosure, tampering, or data loss. Developer: *to be determined after the Firm receives a license.*

c) Secure email system for both external and internal communications. This includes correspondence with clients on AML/CFT-related matters such as onboarding, verification, and clarification of documents, as well as internal communications among staff regarding AML issues, alerts, and reporting obligations. Developer: *to be determined after the Firm receives a license.*

4. Risk-Based Approach

4.1. The Firm is responsible for identifying, assessing, and understanding its exposure to ML/TF risks. Ongoing AML risk management is conducted by the MLRO, or in their absence, the deputy MLRO, with support from other employees as necessary. This process includes:

a) Evaluating relevant risk factors before determining the Firm's overall risk level and corresponding mitigation measures in a manner proportionate to the Firm's nature, size, complexity, and specific ML/TF risk exposure.

b) Maintaining a documented and regularly updated risk assessment.

c) Submitting the risk assessment results for approval by Senior Management in the form of the Business-Wide Risk Assessment (BWRA) report.

d) Establishing mechanisms to provide risk assessment documentation to authorities upon request.

e) Implementing and maintaining key AML controls, including AML compliance oversight, risk assessments (BWRA and Customer Risk Assessment (CRA)), KYC/CDD procedures, transaction monitoring, employee training, recruitment screening (Know Your Employee), and independent audits to ensure system effectiveness.

4.2. When preparing the Business-Wide Risk Assessment (BWRA), the MLRO must identify and assess the Firm's risks in relation to the following factors and determine the overall risk level, along with appropriate mitigation measures:

a) customer base,

b) geographic areas of operation,

c) products or services,

d) delivery mechanisms, channels, or partners,

e) business practices or new product delivery methods, and

f) use of new or emerging technologies.

The BWRA must be reviewed and updated by the MLRO whenever material changes occur in any of the above factors.

4.3. MLRO shall use both quantitative and qualitative data from internal and external sources when conducting BWRA. This includes guidance and reports from the Financial Action Task Force (FATF), and publications issued by AFM, including reports on FATF mutual evaluations and follow-up reports.

4.4. The outcomes of the BWRA must inform the development and effectiveness of AML policies, procedures, systems, and controls; guide resource allocation; and support customer risk assessments.

4.5. The BWRA must be conducted by MLRO and approved by Senior Management at least once a year, before the end of February, and for the first year, prior to the commencement of the Firm's operations.

4.6. Customer Risk Assessment (CRA). The Firm must conduct a risk-based assessment for every customer as part of the onboarding process and update it whenever there is a material change in the customer's circumstances. This includes:

a) Assigning a risk rating based on the customer's exposure to ML/TF risks.

b) Creating a customer risk profile in accordance with the Firm's CRA procedure.

4.7. The CRA must be conducted in parallel with customer due diligence (CDD) and should consider:

a) The identity of the customer, any beneficial owners, and persons acting on their behalf.

b) The purpose and nature of the business relationship.

c) The customer's type, ownership/control structure, and beneficial ownership.

d) The nature and expected activity within the relationship.

e) Country of origin, incorporation, or business location.

f) The type of product or service involved.

g) Whether the customer's activities or the funds amounts align with their declared source of funds and wealth.

h) The results of the Firm's Business-Wide Risk Assessment (BWRA).

4.8. The Firm must understand the business and control structure of any Client that is a legal entity or arrangement. Relationships cannot be established if beneficial ownership cannot be identified due to opaque control structures.

4.9. The Firm must not enter into or maintain relationships with shell banks. A physical presence means having a meaningful mind and management function; merely having a local agent or administrative office is not sufficient.

4.10. MLRO must assign each customer a risk rating such as Low (1–3), Medium (4–7), or High (8–10), based on a documented risk-based assessment of the Client's exposure to money laundering and terrorist financing risks. The risk rating determines the depth of Customer Due Diligence (CDD) required.

4.11. MLRO should consider increasing the risk for the Client, if any of the following apply:

a) The legal services are provided under unusual or opaque circumstances (e.g. use of intermediaries or unexplained urgency).

b) The client is a legal entity or arrangement primarily used for asset holding, such as trusts or private investment companies.

c) Clients that request services for setting up legal entities, nominee structures, or foundations in offshore or low-tax jurisdictions.

d) The client's ownership or control involves bearer shares or nominee shareholders/directors.

e) The client is engaged in a cash-intensive business or where the source of funds is unclear or unverifiable.

f) The client's corporate structure is unduly complex given the nature of the legal work.

g) There is adverse media or other credible public information linking the client to financial crime or reputational risk.

h) The Firm is asked to set up or manage legal vehicles in jurisdictions with weak AML controls.

Service-related and delivery channel risk factors:

a) The relationship or service is conducted non-face-to-face without adequate safeguards (e.g. video verification, e-signature).

b) The engagement involves new, untested, or non-standard legal services, particularly in unregulated digital asset management, or cross-border structuring.

c) The Firm is requested to act as a trustee, nominee, or formation agent without a clear commercial justification.

d) Instructions are provided informally or without written agreement, or involve unusually complex contractual arrangements.

Geographical risk factors:

a) The client (or transaction) has a nexus to jurisdictions:

- With weak AML/CFT systems (identified by FATF or credible sources as high-risk or under increased monitoring);
- Subject to UN, EU, UK, or U.S. sanctions;
- Identified as supporting terrorism or high levels of corruption/criminal activity.

4.12. MLRO should consider lowering the risk for the Client, if they exhibit the following characteristics:

a) A government authority or a publicly owned entity in a jurisdiction with robust AML/CFT standards.

b) A long-standing private individual or corporate client with a transparent history and ongoing relationship with the Firm.

c) A regulated financial institution or listed entity from a country compliant with FATF standards.

Service-related and delivery channel factors for low-risk clients:

a) In-person onboarding with full documentation.

b) Limited-scope legal services such as domestic arbitration or litigation advice.

c) Transparent fee arrangements paid through traceable banking channels.

The assignment of a low-risk rating must be based on a formal CRA. Risk classification must always rely on both the customer's individual profile and the outputs of the Firm's Business-Wide Risk Assessment (BWRA). No risk rating should be automatically assigned.

4.13. The Firm is exclusively engaged in the provision of legal services and does not handle, receive, or execute client financial transactions. As such, transaction-related ML/TF risks are not applicable to the Firm's activities. The Firm's AML/CTF policies, procedures, and controls are therefore focused on non-transactional risk factors, including customer type, jurisdiction, the nature of legal services provided, delivery channels, and other relevant elements consistent with the scope of the Firm's operations.

5. Customer Due Diligence

5.1. The Firm must conduct appropriate Customer Due Diligence (CDD) measures for each of its clients prior to establishing a business relationship and, when necessary, throughout the ongoing relationship. CDD must be conducted to verify the identity of the client, beneficial owners (where applicable), and any persons acting on behalf of the client.

5.2. The Firm must apply Enhanced Due Diligence (EDD) measures in the following cases:

a) Where a client has been assigned a high risk rating under the CRA;

b) Where the client is based in, or associated with, a country or jurisdiction assessed as high risk (e.g., based on FATF guidance, UN sanctions, or other credible sources).

c) EDD measures may include, but are not limited to, obtaining additional information on the client and beneficial owners, enhanced verification of identity, understanding the source of wealth (SOW), source of funds (SOF), and applying enhanced ongoing monitoring procedures.

5.3. The Firm may apply Simplified Due Diligence (SDD) measures where a client is assessed as presenting a low risk of ML/TF, and there is no suspicion of criminal activity.

a) SDD must be commensurate with the low-risk level identified;

b) SDD must not be applied in high-risk scenarios, or where the Firm has any grounds to suspect ML/TF.

5.4. The Firm must complete CDD measures:

a) Before entering into a business relationship with a new client;

b) After establishing a business relationship with a customer.

5.5. The Firm must also conduct appropriate CDD on an existing client if:s

a) There is doubt as to the veracity or adequacy of previously obtained client identification or verification documents;

b) The Firm becomes aware of a suspicion of ML/TF;

c) There is a change in the client's circumstances, nature of engagement, ownership or control structure, or the client’s risk rating;

d) A periodic review is triggered as part of the Firm’s ongoing monitoring procedures.

5.6. The Firm must conduct CDD measures when establishing a business relationship and after its establishment when circumstances warrant a review. Examples include:

a) Emergence of suspicion of ML/TF;

b) A material change in the client's profile or engagement scope that is inconsistent with previously known facts;

c) Indications that the client is acting on behalf of another undisclosed party.

5.7. In conducting CDD, the Firm must:

a) Verify the identity of the client and any authorized representative, including confirmation of such authorization, using original or properly certified documents or reliable, independent sources;

b) Identify and verify any beneficial owners of the Client;

c) Obtain information about and understand the purpose and intended nature of the legal engagement and business relationship;

d) Understand the client's Source of Funds (SOF) to the extent required by the CRA;

e) Understand the client's Source of Wealth (SOW) as per the CRA;

f) Conduct ongoing due diligence over the course of the business relationship to ensure that information remains accurate and up to date.

5.8. Where a customer or a beneficial owner is identified as a PEP, the Firm must:

a) Apply a higher risk rating and increase the degree and frequency of monitoring to detect unusual or suspicious activities.

b) Obtain SEO's approval before establishing the relationship.

If an existing customer or their beneficial owner becomes a PEP, the Firm must not continue the relationship without SEO's approval.

5.9. Specific Requirements for Different Client Types

Natural Persons	Obtain full name, date of birth, nationality, unique identification number, and residential address. Verification should be done using documents such as a national identity card or passport.
Legal Persons and Foreign entities without legal personality	Obtain full legal and trading names, date and place of incorporation or registration, registered address, unique identification number, and principal place of business. Verification should be done using documents such as a certificate of incorporation or tax certificate. Additionally, the Firm must obtain the identity of the directors, partners, trustees, or equivalent persons with executive authority of

	the legal person, as well as any relevant natural person who is a member of the senior management. The Firm must request a valid commercial or professional license from the client, if applicable.
Trusts and Similar Legal Arrangements	Identify the trust by obtaining the name, date of establishment, jurisdiction, unique identification number, and address of the registered office. Verify the identity of trustees, settlors, beneficiaries, and any other persons with control over the trust.

In complying with these requirements, if original documents cannot be obtained, Firm's MLRO should:

a) Obtain a certified copy of identification documents, verified by a person of good standing (e.g., lawyer, notary, chartered accountant, bank manager, police officer, embassy staff, or similar).

b) Download publicly available information from an official source (such as a regulator or government website).

c) Obtain information and research from reliable sources such as reputable companies, information-reporting agencies, banking references, and for low-risk customers, publicly available data on the internet or commercial databases.

d) For increased risk factors, verify the identification information independently through both public and non-public sources.

Understanding Source of Funds (SOF) and Source of Wealth (SOW)

a) SOF: Understanding where funds for a service originate. This can be obtained from the customer during the onboarding process. Firm must keep evidence of the source of funds, such as account opening forms, supporting documents, and customer risk profiles.

b) SOW: Understanding the origin of accumulated wealth, not necessarily in a dollar-for-dollar breakdown, but enough to confirm that wealth is legitimate. For a natural person, this might include information about the source of wealth in an application form or customer questionnaire. This understanding can be supported by documents such as asset titles, audited financial statements, or income tax returns.

5.10. MLRO is responsible for identifying and verifying beneficial owners before entering into any business relationship. This includes:

- Identifying all natural persons who:
    - Directly or indirectly own or control 25% or more of a legal entity.
    - Exercise control through other means (such as voting agreements or board control).

- Hold a senior management role, if no one can be identified under the above two categories.

- For trusts or similar legal arrangements, identifying and verifying all relevant parties: settlors, trustees, protectors, enforcers, beneficiaries (named or otherwise), and anyone entitled to distributions.

- Obtaining and verifying all necessary documents, including:

  - Ownership structure charts and shareholder registers.

  - Certified identity documents and proof of address for each beneficial owner.

  - Documents evidencing control or influence, if applicable.

If a customer is a fund, the MLRO must determine whether it is widely held or closely held. For closely held funds with few investors and significant holdings, all beneficial owners must be identified and verified. In contrast, for widely held retail funds with no material individual control, look-through is not required.

5.11. The Firm shall conduct ongoing monitoring of all business relationships to identify and report suspicious activities by:

a) periodically reviewing the adequacy of the CDD information it holds on customers and beneficial owners to ensure that the information is kept up to date, particularly for customers with a high-risk rating and particularly when:

   a. the Firm changes its CDD documentation requirements;

   b. there is a material change in the business relationship with the customer; or

   c. there is a material change in the nature or ownership of the customer.

5.12. The Firm should undertake a periodic review to ensure that non-static customer identity documentation is accurate and up-to-date. Examples of non-static identity documentation include passport number and residential/business address and, for a legal person, its share register or list of partners. High-risk customers should undergo continuous monitoring and should be reviewed at least once a year, medium-risk customers should be reviewed at least once every two years, and low-risk customers every three years.

a) periodically reviewing each customer to ensure that the risk rating assigned to a customer remains appropriate for the customer in light of the ML/TF risks; and

b) at appropriate times applying CDD to existing customers based on materiality and risk considering whether and when CDD has been previously conducted and the adequacy of the CDD information obtained.

5.13. Where the Firm is unable to conduct or complete the requisite Customer Due Diligence (CDD) in accordance with this AML Policy, it must, to the extent applicable:

a) Not provide legal services or commence a business relationship with the customer;

b) Not continue with the provision of services if an existing relationship is in place;

c) Consider terminating any existing business relationship; and

d) Assess whether the failure to conduct or complete CDD gives rise to grounds for submitting a Suspicious Transaction Report (STR).

5.14. The Firm is prohibited from knowingly dealing with anonymous clients or those using obviously fictitious identities. The above restrictions do not apply in cases where:

a) Compliance with such measures would constitute tipping off, in contravention of applicable AML Regulations; or

b) AFM has provided explicit instructions to act otherwise.

6. Enhanced Due Diligence and Simplified Due Diligence

6.1. The Firm must conduct Enhanced Due Diligence (EDD) where the risk of ML/TF is assessed to be higher. In such cases, and to the extent applicable to the nature of the client relationship, the MLRO must:

a) Obtain and verify additional:

   a. identification information on the customer and any beneficial owner;

   b. information on the intended nature of the business relationship; and

   c. information regarding the rationale for the legal engagement or specific service requested;

b) Update more regularly the CDD information held on the customer and any beneficial owners;

c) Verify information on:

   a. the customer's Source of Funds (SOF); and

   b. the customer's Source of Wealth (SOW), as applicable under the Client Risk Assessment;

d) Increase the degree and nature of monitoring of the business relationship to determine whether the customer's activities or requests appear unusual or suspicious within the context of the legal services provided;

e) Obtain approval of SEO to commence or continue a business relationship with the customer.

6.2. EDD is required in cases where there is a higher risk of ML/TF. This includes, but is not limited to, the following situations:

a) Where the customer has been assessed as ‘high risk’ according to the Firm’s customer risk assessment methodology, including where the customer or beneficial owner is a PEP.

b) Where there are doubts about the authenticity, completeness, or reliability of the information provided by the customer.

c) Where unusual or suspicious activity is detected in the course of the business relationship or transaction monitoring.

d) Where the MLRO determines, based on risk factors or professional judgment, that EDD is appropriate.

6.3. Where the Firm is permitted to apply Simplified Due Diligence measures, modifications to standard Customer Due Diligence (CDD) may include the following adjustments, provided they are proportionate to the customer’s money laundering and terrorist financing risks:

a) Verifying the identity of the customer and identifying any beneficial owners after the establishment of the business relationship.

b) Reducing the frequency of customer identification updates or, where appropriate, not conducting such updates.

c) Deciding not to verify an identified beneficial owner, while still identifying them.

d) Verifying identification documents only by requesting a copy, rather than requiring original or certified versions.

e) Not enquiring into the customer's Source of Funds (SOF) or Source of Wealth (SOW).

f) Not collecting specific information to determine the purpose and intended nature of the business relationship, but instead inferring these from the nature of the established relationship.

The MLRO must ensure that such modifications are proportionate and justifiable based on the specific low-risk profile of the customer. The Firm must not adopt a “one size fits all” approach to low-risk customers. Even where risks are considered low, the level of CDD must reflect the specific risk factors applicable to each case.

6.4. The Firm is always required to identify beneficial owners, except where the customer is a retail investment fund that is widely held or an investment fund with investors contributing via pension schemes. Verification of beneficial owners may be omitted only if the customer is assessed as low risk.

6.5. The Firm rejects establishing a business relationship with clients during onboarding and with existing clients who exhibit potentially higher money laundering risks, including:

a) Client fails to provide necessary data for identity verification or refuse to disclose information for establishing their economic profile.

b) In case there are suspicions that the business relations are being used by the client for the purpose of ML/TF.

c) Clients with unverifiable identities, such as anonymous or knowingly fictitious names.

d) The customer (or its representative) and beneficial owner are listed in Sanctions list.

MLRO must submit STR on such rejections and terminations in accordance with the section 9 of this AML Policy.

Other categories of unacceptable customers are decided case-by-case, considering various factors like applicant's background, economic activity, country of origin, business transactions, and source of funds. MLRO has the authority to make a reasonable decision to refuse to establish or terminate a business relationship with customers. In complex situations the final decision lies with the Firm's MLRO and SEO.

7. Reliance on a Third Party

7.1. The Firm may rely on a third party to conduct one or more elements of Customer Due Diligence (CDD) on its behalf, provided that a contractual agreement is in place. Permitted third parties include:

a) An Authorised Person;

b) A law firm, notary, or other independent legal business, accounting firm, audit firm, or insolvency practitioner, or an equivalent person in another jurisdiction;

c) A Regulated Financial Institution;

d) A member of the Firm's Group.

7.2. The Firm may also rely on CDD information previously obtained by a third party, provided that it covers one or more required elements of the CDD process. The Firm may rely on a third party only to the extent that:

(a) It immediately obtains the necessary CDD information from the third party, including customer and beneficial owner identification and verification documents, and information on the purpose and intended nature of the business relationship or transaction.

(a-a) The third party has undertaken necessary CDD measures, particularly with respect to customer identification and record-keeping.

(b) It takes adequate steps to ensure that certified copies of identification documents used for CDD are available from the third party upon request and without delay. Certification should confirm the document is a "true copy of the original."

(b-a) Regular assurance testing is performed on third-party arrangements to verify the availability, sufficiency, and reliability of CDD documentation.

(c) The third party (under categories (b) to (d)) is subject to AML regulation by a Financial Services Regulator or another competent authority in a jurisdiction with AML standards equivalent to those set by the FATF, and is supervised accordingly.

(d) The third party has not relied on any exception from performing the CDD elements which the Firm intends to rely on.

(e) The information provided is up to date.

7.3. If the Firm is not reasonably satisfied that a customer or beneficial owner has been identified and verified in a manner consistent with its AML rules, it must immediately perform the CDD itself for any deficiencies identified.

7.4. Despite reliance on a third party, the Firm remains fully responsible and liable for ensuring compliance with all CDD requirements under the applicable AML rules. The Firm must ensure that:

a) The third party conducted all necessary CDD and record-keeping measures;

b) The third party has an existing and independent business relationship with the customer;

c) The CDD information received satisfies the Firm's own CDD obligations.

7.5. The Firm must not rely on third parties to perform ongoing monitoring of customers or counterparties concerning AML or sanctions compliance. This rule does not apply to outsourcing or agency relationships governed by section 7.6. of this AML Policy. In such cases, the Firm is responsible for ensuring that:

a) Ongoing due diligence is conducted on the business relationship;

b) The customer's transactions are consistent with the Firm's knowledge of the customer, including its business activities, risk profile, and source of funds.

7.6. The Firm may choose to outsource one or more elements of its CDD to a service provider but will remain responsible for compliance with, and liable for any failure to meet, such obligations. In case of outsourcing, the Firm should conduct appropriate due diligence to assure itself of the suitability of a service provider and should ensure that the provider's obligations are clearly documented in a binding agreement.

8. Sanctions and Findings

8.1. Upon receipt of information outlined in Sections 5.7 and 5.9 of this Policy, the MLRO must promptly conduct a screening of the client, its authorized representatives, and its ultimate beneficial owners (UBOs) against applicable AML Lists, including Sanctions Lists, PEP Lists, and the Firm's Internal

Monitoring List. The results of this screening are used to determine the client's risk rating and to establish the appropriate level of due diligence measures to be applied (SDD, CDD, EDD).

8.2. The MLRO must perform checks using the following publicly available and internal sources:

a) *Sanctions Lists* - This includes individuals and legal entities associated with ML/TF or the proliferation of weapons of mass destruction (WMD). The following resources must be reviewed:
   - **United Nations Security Council Consolidated Sanctions List** available at: https://www.un.org/securitycouncil/sanctions/un-sc-consolidated-list
   - **U.S. Office of Foreign Assets Control (OFAC) - SDN List** Administered by the U.S. Department of the Treasury**.** Available at: https://sanctionssearch.ofac.treasury.gov/
   - **European Union Consolidated Financial Sanctions List** available at: https://www.sanctionsmap.eu/
   - **United Kingdom Consolidated Financial Sanctions List** (HM Treasury) available at: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

b) *Internal Monitoring List* - This list includes individuals and legal entities identified by the Firm as presenting a high ML/TF risk. It includes:
   - MLRO's Monitored List - A list maintained by the MLRO of clients subject to enhanced monitoring due to concerns or suspicions of involvement in ML/TF activities.

d) *PEPs List* - Screening must include identification of individuals who hold or have held prominent public functions, both domestic and international. Sources include:
   - International and public databases for PEP screening, negative news, sanctions, corruption, and bribery by using open-source internet searches and government websites and regulatory announcements in relevant jurisdictions.

8.3. MLRO conducts online ongoing monitoring against the AML Lists (Sanctions List, Internal List and PEP List – as identified in this Policy) published on the corresponding websites before and after onboarding a Client as part of the ongoing monitoring process.

a) **Match with Internal Monitoring List**

If, during the onboarding process, a prospective client is found to match an entry in the Firm's Internal Monitoring List, the MLRO must evaluate the level of risk and consider refusing the establishment of a business relationship. The decision, along with supporting documentation, must be clearly recorded in the prospective client's file.

b) **Match with PEPs List**

If the client or any associated party is identified as a PEP, the client's risk-rating must be increased, and EDD measures must be applied, including but not limited to:

- Senior management approval for onboarding or continuation of the relationship;
- Obtaining and verifying the source of funds and source of wealth;

- Applying enhanced ongoing monitoring procedures.

c) **Ongoing Screening and Monitoring Obligations**

All aforementioned lists (Sanctions, Internal Monitoring, and PEPs) must be checked:

- At onboarding as part of the initial Customer Due Diligence (CDD);
- On an ongoing basis as part of regular CDD and EDD monitoring procedures;
- Whenever a trigger event occurs as identified in this Policy and AML Rules or AML Regulations (e.g., change in client profile, risk rating review, etc).

Ongoing screening must include verification through the afromentioned official websites and tools. The MLRO must maintain documented evidence of all such screening checks in the client's dossier, including the date of screening, source used, findings, and any decisions taken.

8.4. If an existing client is subsequently found to match any entry in the Sanctions List or Internal Monitoring List during ongoing screening, the MLRO must:

- Immediately terminate the business relationship;
- Submit a formal notification to the AFM, providing detailed justification and supporting evidence related to the termination;
- Retain all documentation pertaining to the case, in accordance with internal recordkeeping and regulatory obligations.

8.5. Within one business day of identifying a client on a Sanctions List, MLRO must report to the AFM on actions taken in compliance with the prohibition requirements of relevant United Nations Security Council (UNSC) resolutions or sanctions issued by the UAE, SDN List administered by the OFAC of the U.S. Department of the Treasury, EU Consolidated Financial Sanctions List, UK Consolidated Financial Sanctions List (HMT list), including any onboarding attempts.

8.6. MLRO must immediately notify the Relevant Authorities when it becomes aware that it is:

a) carrying on or about to carry on an activity;

b) holding or about to hold money or other assets; or

c) undertaking or about to undertake any other business, whether or not arising from or in connection with (a) or (b),

for or on behalf of a person, where such action constitutes or may constitute a contravention of a relevant sanction or resolution issued by the UNSC or by the UAE or any a person on Sanctions List as identified in this Policy.

The Firm must report to the Relevant Authorities any actions taken regarding the Customer in compliance with the prohibition requirements of relevant resolutions or sanctions.

8.7. MLRO must ensure that, on an ongoing basis, he/she remains informed of and takes reasonable measures to comply with any findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions (each referred to as a *"Finding"*) issued by the UAE authorities.

8.8. The relevant matters include:

a) arrangements or evaluations regarding the prevention of money laundering or terrorist financing in a particular country or jurisdiction, including any assessment of material deficiency in adopting international standards; and

b) the identification of persons, groups, organizations, or entities where there is a suspicion of money laundering or terrorist financing.

8.9. MLRO must immediately notify the Relevant Authorities in writing if it becomes aware of non-compliance by any person with a Finding and must provide sufficient details regarding the person concerned and the nature of the non-compliance.

9. Reporting to AFM on STRs

9.1. When the Firm's MLRO receives a notification based on section 3.8 of this AML Policy, the MLRO, without delay:

(a) enquires into and documents the circumstances surrounding the notification;

(b) determines whether a Suspicious Transaction Report (STR) must be made to the AFM and documents such determination; and

(c) if required, submits an STR to the AFM and promptly notifies the Relevant Authorities of such a submission.

9.2. Where, following a notification to the MLRO, no STR is made, the MLRO must record the reasons for not making an STR.

9.3. Whether the MLRO decides to make or not to make an STR, the decision shall be made independently and is not subject to the consent or approval of any other person.

9.4. Where the Firm's MLRO has a suspicion of money laundering and reasonably believes that performing the CDD process will tip off the customer, they must not pursue the CDD process and must submit an STR to the AFM.

9.5. All employees, and particularly the MLRO, must be aware that the failure to report suspicions of money laundering or terrorist financing may constitute a criminal offence under applicable laws and regulations.

10. Reporting to Relevant Authorities

10.1. The Firm must complete the AML Return form on an annual basis and submit it to the Relevant authorities (if applicable) within two (2) months after the end of each calendar year.

10.2. The AML Return must be accurate, complete, and reflect the Firm's AML/CFT risk assessment, policies, procedures, and activities. The MLRO is responsible for preparing and reviewing the submission, ensuring timely delivery and compliance with the Relevant authorities' regulatory requirements.

10.3. The MLRO must maintain a log of all submitted STRs, including the date of submission, the reason for reporting, the transaction or client involved, and any follow-up actions taken. This log must be securely stored and made available to the Relevant Authorities or other competent authorities upon request.

10.4. Unless otherwise directed by Relevant Authorities, in accordance with AML Rules 14.4.1, the Firm must inform the Relevant Authorities in writing quarterly about number, reasons, and outcomes if, in relation to its activities carried on, it:

a) Receives an ad-hoc (specific) request from a regulator or agency responsible for AML/CFT or sanctions compliance, requesting detailed information about a specific customer or transaction in relation to potential money laundering or a sanctions contravention;

b) Becomes aware, or has reasonable grounds to believe, that a money laundering event has occurred or may have occurred in or through its business;

c) Becomes aware of any money laundering or sanctions-related matter in relation to the Firm or a member of its Group that could result in adverse reputational consequences;

d) Becomes aware of a significant contravention of the AML Rules or of relevant legislation of the UAE by the Firm or any of its employees.

11. Training and Awareness

11.1. It is mandatory for all Employees to comply with the AML Regulations and the Firm's AML Policy. All Employees are required to participate in AML training sessions provided by the MLRO. Following the training, employees must successfully complete an AML test to demonstrate their understanding of the training material. Failure of completing or providing correct response to the 70% of the test questions should lead to disciplinary actions by the Firm as identified in this AML Policy.

11.2. To ensure high standards when hiring employees, the Firm implements thorough Know Your Employee (KYE) screening procedures. This includes verifying by HR or MLRO the identity of the Employee, conducting criminal and financial background checks, and screening candidates against Sanctions and PEP lists. Employment history, qualifications, and references will be verified, and a risk assessment will be conducted based on the candidate's role and potential exposure to sensitive financial activities. Ongoing monitoring is also conducted by HR or MLRO to ensure employees remain compliant with AML regulations throughout their tenure, including regular sanctions list checks.

11.3. AML training sessions provided by the MLRO should ensure that the Employees:

a) are made aware of the law relating to money laundering;

b) are regularly given training on how to recognize and deal with activities that may be related to money laundering;

c) understand the Firm's policies, procedures, systems, and controls related to money laundering, as well as any changes to these;

d) understand the types of activity that may constitute suspicious activity in the context of the business in which an employee is engaged and that may warrant a notification to the MLRO;

e) understand the arrangements regarding the making of a notification to the MLRO;

f) are aware of the prevailing techniques, methods, and trends in money laundering relevant to the business of the Firm;

g) understand the risk of tipping off and how to avoid informing a customer or potential customer that it is or may be the subject of a Suspicious Transaction Report (STR);

h) understand the roles and responsibilities of employees in combating money laundering, including the identity and responsibility of the Firm's MLRO and deputy, where applicable; and

i) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions related to money laundering.

The relevant training records must be kept for six years after the training has been conducted.

12. Data Protection and Audit

12.1. The Firm's MLRO must:

a) verify if there is secrecy or data protection legislation that would restrict access to the records referred to in its policies, procedures, and controls by the Firm, the Relevant Authorities, or applicable law; and

b) where such legislation exists, obtain certified copies of the relevant records without delay and store these copies in a jurisdiction that allows access by those persons identified in (a).

12.2. The Firm must ensure that its audit function (internal or external) includes regular reviews and assessments (at least once every two years) of the effectiveness of the Firm's policies, procedures, systems, and controls, and its compliance with relevant obligations.

12.3. The review and assessment may be undertaken:

12.4. internally by the Firm’s internal audit function; or

12.5. by a competent firm of independent auditors or compliance professionals.

12.6. The review and assessment should cover at least the following:

12.7. sample testing of compliance with the Firm’s customer due diligence (CDD) arrangements;

12.8. the adequacy of the Firm's AML systems, the ML/TF risk assessment framework, and the application of a risk-based approach;

12.9. the effectiveness of the system for recognizing and reporting suspicious transactions;

12.10. an analysis of all notifications made to the MLRO to highlight any areas where procedures or training may need to be enhanced;

12.11. a review of the nature and frequency of the dialogue between senior management and the MLRO; and

12.12. the level of awareness of staff with AML/CFT responsibilities.

12.13. The resulst of such review and assessment must be reviewed by the MLRO and presented to the Senior Management. If any breaches are found, within two months of receiving such report, MLRO must create an action plan in order to eliminate the breaches.

13. Recordkeeping

13.1. The following information and documents shall be recorded and stored electronically and/or on paper in the dossier:

a) Originals and copies of documents, extracts from databases containing information from available sources, and written information obtained while implementing the Firm’s AML Policy. This includes documents related to customers (including their representatives and beneficial owners) and records obtained throughout the CDD and ongoing monitoring process, such as constituent documents, identity documents, and documents confirming representatives' authorities, information and proofs of source of wealth and source of funds, etc. These documents and information, including information about Clients, their representatives, beneficial owners, counterparties, and agreements with the Firm, shall be retained for a period of 6 (six) years after the termination of business relations.

b) Other documents containing information about the Clients, representatives and beneficial owners, obtained as a result of implementing the Firm’s AML Policy, including business correspondence with the Client and documents confirming the reasons for refusing to establish, continue, or terminate business relations, shall be kept in the legal file of the Client for a period of 6 (six) years from the date of terminating relations with the Client.

c) Messages from Employees/structural units, along with documents resulting from the MLRO's investigation on suspicious, unusual activities, or activities corresponding to the typologies, schemes, and methods of ML/TF approved by the AFM, along with supporting documents, are to be stored in electronic form for 6 (six) years from the date of deciding to recognize the activity as suspicious and sending relevant messages to the AFM.

d) Electronic messages on transactions subject to financial monitoring sent by the Firm to the AFM and notifications to the Relevant Authorities's AML Department shall be stored in electronic form in the recordkeeping system of the Firm for 6 (six) years from the date of sending.

e) Requests from the authorities for the provision of information and documents related to AML issues, as well as responses to such requests, are to be kept by the MLRO for at least 6 (six) years from the date of receiving/submitting the response to such requests.

f) Documents certifying that the MLRO and other employees has completed AML training are to be kept in the employee's personal file during the entire period of their employment in the Firm and after the termination of employment or outsourcing contract for the period of at least 6 (six) years.

g) Any other information and documents regarding the AML procedures as required by AML Regulations.

13.2. The Relevant Authorities may, by notice in writing, require it to keep the records relating to a specified customer for a period specified by the such Authorities that is longer than those referred in this Policy, where the records are relevant to an ongoing criminal or other investigation, or to any other purposes as specified in the notice. In such cases those records shall be kept for the period specified by Authorities.

14. Violations and Disciplinary Actions

14.1. Upon detection of a violation or a likelihood of a violation of AML Regulations and/or AML Policy by Employees, an Employee or a line manager immediately informs the MLRO by available written means of communication (by email/chats that can be retained, providing hard copies of documents).

14.2. Violations of the AML Regulations and/or AML Policy are:

a) Informing Clients and their representatives about sending information about their suspicious activities to the AFM by employees.

c) Failure to take measures by Employees for due diligence of Clients (their representatives), beneficial owners, counterparties.

d) Failure to provide or providing untimely information to the MLRO by Employees on the refusal to establish business relations, termination of business relations with a Client for AML-related reasons.

f) Establishing business relations with PEPs without the written permission of the SEO of the Firm.

h) Failure to send notifications of suspicious/unusual activities for consideration by the MLRO.

i) Failure to send or sending untimely messages by the MLRO to the AFM about suspicious activities, refusals to establish business relations or terminate business relations with a client.

j) Non-compliance by Employees or the MLRO with the recordkeeping requirements of information and documents.

k) Any other violations occurring during the implementation of the AML Policy.

14.3. Information about violations of the applicable AML Regulations must be communicated to the MLRO and/or the Senior Management using any available means of written communication.

14.4. Employees who violate the AML Policy may be subject to disciplinary action, the severity of which will depend on the nature of the violation. Disciplinary measures may include:

a) reprimand

b) demotion

c) suspension

d) termination

e) the reduction of benefits for a specified or indefinite period

f) for unlawful acts - legal action against the Employee.

Employees should be aware that a serious failure to comply with the AML Regulations or AML Policy may result in regulatory action not only against the individual employee but also against the Firm, its managers, or MLRO. Such regulatory consequences may arise from a single serious incident or from a pattern of persistent or concerning conduct.

15. Final provisions

15.1. This Policy is effective immediately at the date of approval. The Policy may be amended and supplemented as the requirements of the AML Regulations change, as well as the revision of methods of managing ML/FT risks in the Firm.

15.2. In case of amendments to the AML Regulations, if the amendments affect the Firm’s requirements or activities, MLRO must make the appropriate amendments to the AML Policy or documents within thirty 30 calendar days. Amendments to the AML Policy shall be presented and approved by the Firm’s Shareholder(s) resolution.

15.3. The provisions not regulated by the Policy are regulated by the AML Regulations and applicable Relevant Authorities guidance and AFM orders.

15.4. In the event of amendments in the AML Regulations and a conflict between certain provisions of this Policy and the AML Regulations, such provisions of the Policy become invalid, and the Firm employees are guided in their activities by the applicable AML Regulations until the relevant changes are made.