



QUANTUM FAMILY OFFICE

INTERNATIONAL TRUST-SERVICES



Anti-Money Laundering and Countering the Financing of Terrorism Policy

As required by the Law of Bulgaria Art. 9A, paragraph 1 of the "LAW ON MEASURES AGAINST MONEY LAUNDERING IN THE PUBLIC REGISTER OF PERSONS WHO BY OCCUPATION ARE ENGAGED IN EXCHANGE SERVICES BETWEEN VIRTUAL CURRENCIES AND FIAT CURRENCIES AS WELL AS CUSTODIAN WALLET PROVIDERS".

I. Introduction

1. The Anti-money laundering and countering the financing of terrorism policy (the "AML/CFT Standards" or "Standards") are developed to implement the Anti-Money Laundering and Countering the Financing of Terrorism Policy (the "AML/CFT Policy") as required by the Law of Bulgaria "ON MEASURES AGAINST MONEY LAUNDERING IN THE PUBLIC REGISTER OF PERSONS WHO BY OCCUPATION ARE ENGAGED IN EXCHANGE SERVICES BETWEEN VIRTUAL CURRENCIES AND FIAT CURRENCIES AS WELL AS CUSTODIAN WALLET PROVIDERS ". These AML/CFT Standards set the minimum and mandatory benchmarks to prevent, detect, and investigate money laundering and financing of terrorism, and to control and manage related risks (collectively referred to as "ML/FT Risks").

1.1 Objectives

2. The AML/CFT Standards are intended to establish effective measures comparable to international best practice to enable QUANTUM FAMILY-OFFICE to achieve the objectives established in the AML/CFT Policy, which are:

- (a) Preventing the abuse of THE COMPANY resources for money laundering ("ML") and/or financing of terrorism ("FT");
- (b) Meeting applicable legal requirements and international standards in jurisdictions where THE COMPANY and its Counterparties operate.
- (c) Mitigating any reputational risk.
- (d) Supporting the establishment and/or strengthening of capacities in countries to meet THE COMPANY's fiduciary standards regarding AML/CFT.
- (e) Guarding against establishing any relations or undertaking any transaction that may relate to or may facilitate ML and/or FT or any other illicit activity.
- (f) Exercising due diligence when dealing with Counterparties, persons appointed to act on behalf of Counterparties, and connected parties of the Counterparties; and
- (g) Continuously reviewing and updating its AML/CFT Policy and its corresponding AML/CFT Standards as threats and international standards evolve to prevent and detect ML and/or FT.

3. These AML/CFT Standards further aim to meet the expectation of international contributors and other key stakeholders that THE COMPANY complies with all its policies; takes appropriate measures to prevent corrupt, fraudulent, and otherwise illegal practices, including the prevention of the use of THE COMPANY resources to finance terrorist activity; and adopts best practice fiduciary principles and standards relating to anti-corruption, countering of financing of terrorism, fraud, and anti-money laundering, as reflected in contribution agreements/ arrangements.

4. In pursuing these purposes and objectives, these AML/CFT Standards intend to prevent that THE COMPANY is exposed to serious reputational damage, financial loss, or legal liability, which may give rise to strong challenge by international contributors, donors, and other key stakeholders.

5. The provisions of the AML/CFT Policy and the Standards shall be applied coherently and in accordance with the scope of THE COMPANY AML/CFT Policy, across all relevant procedures, methodologies and templates including the Accreditation Master Agreements.

1.2 Scope

6. This Policy set out specific obligations for THE COMPANY Personnel in accordance with their roles and responsibilities with respect to THE COMPANY and requirements defined by the Law of Bulgaria "ON MEASURES AGAINST MONEY LAUNDERING IN THE PUBLIC REGISTER OF PERSONS WHO BY OCCUPATION ARE ENGAGED IN EXCHANGE SERVICES BETWEEN VIRTUAL CURRENCIES AND FIAT CURRENCIES AS WELL AS CUSTODIAN WALLET PROVIDERS".

7. THE COMPANY shall apply these Policy standards to potential and existing Counterparties in accordance with the provisions of the AML/CFT Policy.

II. Definitions

9. For the purposes of these Standards, the following definitions shall be applied:

- (a) **"AML/CFT Program"** refers to the overall ML/FT risks control and management components, including governance and oversight and the establishment of an Integrity Risk Management Group, Counterparty due diligence, risk assessment, financial activities monitoring, suspicious activities reporting, the AML/CFT Policy, the AML/CFT Standards, compliance, training, and record keeping.
- (a) **"Bearer Negotiable Instruments (BNIs)"** refer to monetary instruments in bearer form such as: traveler's cheques; negotiable instruments (including cheques, promissory notes, and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including cheques, promissory notes, and money orders) signed but with the payee's name omitted.
- (b) **"Bearer Shares"** refer to negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate.
- (c) **"Beneficial Owner"** means the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.
- (d) **"Beneficiary"** refers to the person or persons who are entitled to the benefit of any trust arrangement. A beneficiary can be a natural or legal person or arrangement. In the context of life insurance or another investment-linked insurance policy, a beneficiary is the natural or legal person, or a legal arrangement, or category of persons, who will be paid the policy proceeds when/if an insured event occurs, which is covered by the policy.

- (f) **"Competent Authorities"** refer to all public authorities (including financial supervisors established as independent non-governmental authorities with statutory powers) with designated responsibilities for combating money laundering and/or terrorist financing. In particular, these include the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency; and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and Designated Non-Financial Businesses and Professions with AML/CFT requirements.
- (h) **"Correspondent Banking"** is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts, and foreign exchange services;
- (i) **"Counterparty"** is any party that contributes to, executes, implements, bids for, or in any way participates in Company-related Activities, including receiving a grant, loan, or other form of financing or support from the Company. Counterparties include a contributor, Accredited Entity, Direct Access Entity, Executing Entity, delivery partner, fiscal agent, financial intermediary, vendor, and (for the purpose of the AML/CFT Policy) any entity within or to which the Executive Director directly disburses THE COMPANY resources, including for the Readiness and Preparatory Support Program.
- (j) **"Designated Non-Financial Businesses and Professions (DNFBP)"** mean:
- (i) Casinos, including internet- and ship-based casinos.
 - (ii) Real estate agents.
 - (iii) Dealers in precious- or strategic metals.
 - (iv) Dealers in precious stones.
 - (v) Lawyers, notaries, other independent legal professionals and accountants (this refers to professionals within professional firms, not 'internal' professionals);
 - (vi) Trust and Company Service Providers refer to all persons or businesses providing any of the following services to third parties:
 - (1) Acting as a formation agent of legal persons.
 - (2) Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons.
 - (3) Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement.

- (4) Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement; and
 - (5) Acting as (or arranging for another person to act as) a nominee shareholder for another person).
- (k) **"Financial Institutions"** mean any natural or legal person who conducts as a business one or more of the following activities or operations for or on behalf of a customer:
 - (i) Acceptance of deposits and other repayable funds from the public.
 - (ii) Lending.
 - (iii) Financial leasing.
 - (iv) Money or value transfer services.
 - (v) Issuing and managing means of payment (e.g., credit and debit cards, cheques, traveler's cheques, money orders and bankers' drafts, electronic money);
 - (vi) Financial guarantees and commitments.
 - (vii) Trading in:
 - (1) Money market instruments.
 - (2) Foreign exchange.
 - (3) Exchange, interest rate, and index instruments.
 - (4) Transferable securities; and
 - (5) Commodity futures trading (it does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds).
 - (viii) Participation in securities issues and the provision of financial services related to such issues.
 - (ix) Individual and collective portfolio management.
 - (x) Safekeeping and administration of cash or liquid securities on behalf of other persons.
 - (xi) Otherwise investing, administering, or managing funds or money on behalf of other persons.
 - (xii) Underwriting and placement of life insurance and other investment-related insurance; and
 - (xiii) Money and currency changing.
- (n) **"Foundation"** refers to a non-governmental entity that is established as a non-profit corporation or a charitable trust, with a principal purpose of making grants to unrelated organizations, institutions, or individuals for scientific, educational, cultural, religious, or other charitable purposes. There are two types of foundations:

- (i) Private Foundation derives its money from a family, an individual, or a corporation; and
 - (ii) Grant-making Public Charity (sometimes referred to as a "Public Foundation") derives its support from diverse sources, which may include foundations, individuals, and government agencies.
- (p) **"THE COMPANY Personnel"** means any THE COMPANY Staff and any other individual contracted and/or engaged by THE COMPANY to perform official functions for THE COMPANY.
- (s) **"Money Laundering"** means the conversion or transfer of property, knowing that such property is derived from crime, for the purposes of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions. It is the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing such property is derived from crime, or the acquisition, possession, or use of property, knowing at the time of receipt that such property was derived from a criminal offence.
- (t) **"Money or Value Transfer Service (MVTs)"** refers to financial services that involve the acceptance of cash, cheques, other monetary instruments, or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTs provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party and may include any new payment methods. Sometimes these services have ties to geographic regions and are described using a variety of specific terms, including Hawala, Hundi, and Feichen.
- (u) **"Non-Profit Organization (NPO)"** refers to a legal person or arrangement or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social, or fraternal purposes, or for the carrying out of other types of "good works".
- (v) **"Political Exposed Person (PEP)"** refers to individuals who are or have been entrusted (domestically or by a foreign country) with prominent public functions, such as Heads of State or of government; senior politicians; senior government, judicial, or military officials; senior executives of state-owned corporations; and important political party officials. It also refers to persons who are or have been entrusted with a prominent function by an international organization, which includes members of senior management such as directors, deputy directors, members of a Executive Director, or persons who hold equivalent functions. The definition is not intended to cover middle ranking or relatively junior individuals in the foregoing categories. Immediate family members of

PEPs (such as spouses, children, parents, and siblings) or close associates of PEPs (such as widely and publicly-known close business colleagues and/or personal advisors, in particular financial advisors or persons acting in a fiduciary capacity) are also included in this category as the same risks are involved as with PEPs themselves.

- (w) **“Prohibited Practices”** are specific conduct such as Corrupt Practice, Fraudulent Practice, Coercive Practice, Collusive Practice, Obstructive Practice, Abuse, Retaliation against Whistleblowers or Witnesses, Money Laundering, and Terrorist Financing.
- (x) **“Shell Bank”** refers to a bank that has no physical presence in the country in which is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low-level staff does not constitute physical presence.
- (y) **“Staff”** means all persons appointed to a post in THE COMPANY under a letter of appointment (individually, a “Staff Member”).
- (z) **“Suspicious Activity”** refers to any activity conducted by Counterparties, whether with monetary value or not, with connection to THE COMPANY in whatsoever manner, and that such activity appears to have connection with money laundering, the financing of a terrorist activity, or other Prohibited Practice or criminal offence.
- (aa) **“Suspicious Activity Report (SAR)”** means a report concerning a Suspicious Activity which is made to the Head of AML / CFT COMPLIANCE OFFICER for investigation and/or disclosure to Competent Authorities.
- (bb) **“Terrorist Financing”** is defined as the commission of any offence as set out in Article 2 of the *International Convention for the Suppression of the Financing of Terrorism*.
- (cc) **“Tipping-off”** means disclosing the fact to a Counterparty that a Suspicious Activity or related information is filed with THE COMPANY management or Competent Authorities in relation to a Company-related Activity; and
- (dd) **“Trust”** refers to the legal relationships created – *inter vivos* or on death - by a person, the settlor, when assets have been placed under the control of a trustee for the benefit of a beneficiary or for a specified purpose. A trust has the following characteristics:
 - (i) The assets constitute a separate fund and are not a part of the trustee's own estate.
 - (ii) Title to the trust assets stands in the name of the trustee or in the name of another person on behalf of the trustee.
 - (iii) The trustee has the power and the duty, in respect of which he is accountable, to manage, employ, or dispose of the assets in accordance with the terms of the trust and the special duties imposed upon him by law; and
 - (iv) The reservation by the settlor of certain rights and powers, and the fact that the trustee may himself have rights as a beneficiary, are not necessarily inconsistent with the existence of a trust. Settlor refers to natural or legal persons who transfer ownership of their assets to trustees by means of a trust deed or similar arrangement.

III. Roles and Responsibilities

10. All **THE COMPANY Personnel** are responsible for:

- (a) Complying with the AML/CFT Policy, these AML/CFT Standards, and controls of THE COMPANY.
- (b) Familiarizing themselves and acting in accordance with relevant THE COMPANY processes and procedures to manage AML/CFT compliance; and
- (c) Reporting to the AML / CFT COMPLIANCE OFFICER without undue delay any suspected ML/FT activity, any Suspicious Activity, or red flag (indicator of Suspicious Activity).

IV. AML/CFT Risk Management

15. THE COMPANY shall ensure that ML/FT risks are effectively managed to mitigate exposure to reputational, financial, and legal risks, as well as to protect its operations and the integrity of its resources and activities.

16. At minimum, ML/FT risk management of THE COMPANY shall include:

- (a) A fit-for-purpose AML/CFT Program to control and manage ML/FT risks in an effective manner, including the establishment of the Integrity Risk Management Group.
 - (b) An annual Institutional Risk Assessment, conducted under the supervision of the AML / CFT COMPLIANCE OFFICER, designed to identify the residual¹ risks to which THE COMPANY is exposed and to assess the effectiveness of the overall AML/CFT Program.
 - (c) Assurances that the AML/CFT Standards and SOPs are executed and complied with effectively, including a Risk Control Self-Assessment ("RCSA") tool² to measure the completeness and level of compliance of the standards and procedures.
-

- (d) An annual AML/CFT compliance review to test the effectiveness of AML/CFT controls and to formulate appropriate action plans to address identified control and compliance gaps; and
 - (e) AML/CFT theme audits as required.
17. The Executive Director shall ensure that outcomes and any risks or deficiencies of the assessments, reviews, and audits specified in paragraph 16(b) to (e) are reported to the ED, the AML / CFT COMPLIANCE OFFICER, and relevant divisions/offices of the Executive Director.

V. Assessing Risk and Risk-Based Approach

18. THE COMPANY shall take all reasonable measures to identify, assess, and understand ML/FT risks, document those assessments, and apply resources to ensure the risks are managed and mitigated effectively. For this purpose, THE COMPANY shall adopt and implement a continuous risk-based approach to ensure that measures to prevent or mitigate ML and FT are commensurate with the risks identified. Following the risk-based approach, THE COMPANY shall implement an annual Institutional Risk Assessment to identify and understand ML/FT residual risks in its operations with a view to enhancing its systems and controls for risk mitigation and resource distribution in overall AML/CFT control and management.

VI. Counterparty Due Diligence

6.1 THE COMPANY Counterparty Due Diligence Terms

19. In accordance with Anti-money laundering and countering the financing of terrorism policy, THE COMPANY shall apply Counterparty Due Diligence ("CDD") measures, as determined in accordance with the risk-based approach, considering the type of Counterparty, Counterparty relationship, financial instrument, and country of operation, and shall identify and verify the identity of the Counterparties (including their Beneficial Owners) with which THE COMPANY enters into a Counterparty relationship. Further, THE COMPANY shall take reasonable measures to duly assess the purpose, economic rationale, and overall AML/CFT and related integrity aspects of the Counterparty and its Beneficial Owners to avoid being involved in relationships structured for the purposes of ML and FT.

20. Pursuant to paragraph 19 above, THE COMPANY shall assess ML/FT risks in potential or existing Counterparty relationships through a risk assessment methodology and process.

21. In conducting risk assessments, THE COMPANY shall establish guidance in the AML/CFT to assist in determining the level of risk posed by a potential or existing Counterparty taking into account the types of persons or entities which may present elevated ML/FT risks according to international standards set by the FATF. These include but are not limited to:

- (a) Politically Exposed Persons (PEP) including their immediate family members or close associates, or PEP-linked entities.
- (b) Financial Institutions providing Correspondent Banking or Money or Value Transfer Services (MVTs).

- (c) Designated Non-Financial Businesses and Professions.
- (d) Entities issuing Bearer Shares or with nominee shareholders or directors.
- (e) Trusts.
- (f) Entities with unduly complex structure³ of ownership; and
- (g) Non-Profit Organizations (NPOs).

22. THE COMPANY shall undertake appropriate Know-Your-Counterparty ("KYC") measures in entering any relationship with a potential or existing Counterparty. KYC measures shall include identifying and verifying the full identity of the Counterparty and the authenticity of that information.

23. Following the risk-based approach, THE COMPANY may apply more stringent or more specific KYC measures with regard to potential or existing Counterparties which are assessed in any one of the categories identified in paragraph 21(a) to (g). In particular, the Beneficial Owner(s) of a Counterparty must be identified and verified.

24. CDD information and identification evidence must be obtained directly from the potential or existing Counterparty, or from independent and reliable sources, such as public records maintained by the relevant government or relevant government-connected sources, the potential or existing Counterparty's official website, publication or public materials, or, in exceptional cases, on-site visits by THE COMPANY Personnel or appointed third parties. Information from public web search platform or telephone calls may be referenced but will not be considered as independent and reliable sources for verification purposes.

25. THE COMPANY shall ensure that all potential and existing Counterparties are screened in accordance with paragraphs 14 (a) and (b) of the AML/CFT Policy.

26. THE COMPANY shall ensure that CDD is to be completed before entering into a contractual relationship with a Counterparty. Under no circumstance shall disbursements be made before CDD is completed and approved.

27. THE COMPANY shall ensure ongoing AML/CFT monitoring after a Counterparty has been on Executive Directed following the risk-based approach. At minimum, such measures shall include ensuring CDD data is up-to-date and monitoring that Company-related Activities undertaken by Counterparty are in accordance with contractually agreed terms, and that THE COMPANY Funds are not being misused for ML/FT activities. Counterparties shall be required to inform THE COMPANY of any changes regarding CDD information when they become aware of such changes and without undue delay.

28. THE COMPANY shall ensure that periodic CDD reviews of Counterparties are conducted so that emerging risks may be identified early, minimizing any undue consequences and impact to THE COMPANY. The CDD review cycle shall be determined through the risk-based approach.

29. THE COMPANY will refrain from establishing new relationships with entities and will terminate existing Counterparty relationships in accordance with the AML/CFT Policy.

30. Pursuant to paragraph 29 above and in accordance with paragraph 8 of the AML/CFT Policy which states that the Policy shall be consistent with the relevant United Nations Conventions and Recommendations of the FATF, THE COMPANY shall refrain from engaging with potential or existing Counterparties which are found to be:

³ Unduly complex structure means that a complex structure has been put in place for no apparent purpose, suggesting that it is mainly there to disguise the beneficial owners.

- (a) Shell banks, unlicensed banks, or unregulated Money or Value Transfer Service (MVTs) providers or agents.
 - (b) Engaged in relationships with (have dealings with or provide services to) shell banks, unlicensed banks, or unregulated MVTs providers or agents.
 - (c) Engaged in relationships with other entities which engage in relationships with shell banks, unlicensed banks, or unregulated MVTs providers or agents for the purposes of implementing a Company-related Activity.
 - (d) Disbursing funds, directly or indirectly, through Cash Couriers for the purposes of implementing a Company-related Activity.
 - (e) Financial Institutions that issue Bearer Shares; and
 - (f) Financial Institutions that keep anonymous accounts or accounts in fictitious names for their clients.
31. In addition, THE COMPANY shall not allow fund disbursements to anonymous, numbered accounts or passbooks, or third-party accounts, under any circumstances.
32. Pursuant to paragraphs 29 and 30 above, the list of unacceptable relationships may be expanded or amended in line with the changing environment.

6.2 Reliance on Accredited Entities and Delivery Partners to Perform CDD on Underlying Counterparties

33. THE COMPANY shall rely on Accredited Entities and Delivery Partners to identify and mitigate risks of ML/FT in deploying and managing THE COMPANY resources. To that end, THE COMPANY relies on Accredited Entities and Delivery Partners to perform due diligence on their underlying potential or existing counterparties and to ensure AML/CFT record-keeping in accordance with their policies and procedures.
34. THE COMPANY shall take steps to ensure appropriate due diligence will be applied to Accredited Entity's or Delivery Partner's underlying potential or existing counterparties in Company-related Activities, and that the AML/CFT measures taken by Accredited Entity or the Delivery Partner to identify ML/FT risks are effective.
35. Following the execution of any contractual agreement with an Accredited Entity, THE COMPANY shall monitor that the Accredited Entity or Delivery Partner applies effective AML/CFT measures in any Company-related Activity. Such monitoring may include requesting that Accredited Entities and Delivery Partners make available copies of identification data and other due diligence documents without undue delay, and other appropriate examination actions as required. It also may include monitoring actions and proactive integrity reviews conducted by the AML / CFT COMPLIANCE OFFICER.

VII. Financial Transaction Activities Monitoring

36. In accordance with this Anti-money laundering and countering the financing of terrorism policy, THE COMPANY shall establish processes for monitoring financial transaction activities and reporting Suspicious Activities. At minimum, THE COMPANY shall undertake a number of informed measures (to be elaborated in the SOPs) following the risk-based approach including but not limited to:
- (a) Setting criteria for or providing guidance to Counterparties for the selection of Financial Institutions or financial intermediaries through which THE COMPANY Funds are disbursed from

THE COMPANY to end recipients or beneficiaries. Such criteria include financial transaction monitoring and reporting.

- (b) Setting criteria for and requiring the extent to which Counterparties report regularly to THE COMPANY on their underlying financial transactions in Company-related Activities; and
- (c) Developing tools to analyze reported financial transactions, regularly reviewing the continuing effectiveness of the tools and, where necessary, initiating any enhancements or changes.

VIII. Reporting Red Flags, Suspicious Activities, and Suspected ML/FT

37. THE COMPANY Personnel/Individuals shall report any Suspicious Activity, red flag (indicators of a suspicious activity), or ML/FT activity which they identify or suspect in the course of performing their duties to the AML / CFT COMPLIANCE OFFICER for investigation. Such reports shall be made and investigated in accordance with THE COMPANY policies and procedures. Failure to report may leave THE COMPANY open to serious reputational damages or legal liability.

38. The AML / CFT COMPLIANCE OFFICER shall take appropriate measures to enable the reporting of red flags, Suspicious Activities, or ML/FT activities directly to the AML / CFT COMPLIANCE OFFICER by raising awareness and by providing easily accessible reporting channels. The AML / CFT COMPLIANCE OFFICER shall ensure that all reports of red flags, Suspicious Activities, and suspected ML/FT activities reports are documented, attended to, and investigated in a prompt and professional manner.

39. The AML / CFT COMPLIANCE OFFICER shall notify THE COMPANY Executive Director when a Suspicious Activity or suspected ML/FT activity has been substantiated pursuant to an AML / CFT COMPLIANCE OFFICER investigation. THE COMPANY Executive Director shall determine to disclose that Suspicious Activity or suspected ML/FT activity to a Competent Authority of a country where the Suspicious Activity takes place in accordance with THE COMPANY policies and procedures. THE COMPANY may authorize the AML / CFT COMPLIANCE OFFICER to make a disclosure on behalf of THE COMPANY. Decisions to disclose or not to disclose Suspicious Activities and suspected ML/FT activities must be clearly recorded and reported. Procedures for disclosing Suspicious Activities and suspected ML/FT to Competent Authority shall be developed by the AML / CFT COMPLIANCE OFFICER in coordination with THE COMPANY Executive Director.

40. In accordance with THE COMPANY policies, rules, and procedures, THE COMPANY may take disciplinary or other remedial action against any THE COMPANY Personnel who, having knowledge of Suspicious Activities, fails without reasonable excuse, to make a report, or who blocks, or attempts to block, a report by another THE COMPANY Personnel.

41. Under no circumstances should THE COMPANY Personnel engage in Tipping-off. Engaging in Tipping-off could prejudice an existing or potential investigation by the AML / CFT COMPLIANCE OFFICER or Competent Authorities and may be subject to remedial action in accordance with THE COMPANY policies on ethics and conflicts of interest, and with regard to THE COMPANY Personnel, other relevant policies and procedures of the Company.

IX. Exiting a Relationship

42. It is the policy requirement of this AML/CFT Policy for THE COMPANY not to enter into or maintain relationships with Counterparties that are being used for money laundering or terrorist financing. Guidelines on exiting a relationship shall be developed by the Executive Director of the Company.

X. Training and Capacity Building

43. THE COMPANY shall ensure that THE COMPANY Personnel receive adequate AML/CFT training which aims to strengthen their knowledge and awareness of the following subject matter:

- (a) The relevant obligations, requirements, rules, and procedures set out in this AML/CFT Policy, Standards, and in related THE COMPANY policies and guidelines, and the possible consequences for compliance failures; and
- (b) Information and methods useful for identifying and procedures for reporting ML/FT, red flags, Suspicious Activities, and other related integrity risks or violations.

44. To give effect to AML/CFT training, THE COMPANY shall develop and implement AML/CFT training guidelines. Such guidelines should address, at minimum, the frequency, content, methods, and knowledge testing of the training and consequences for failure to undergo or complete the training and should be designed for THE COMPANY Personnel in consideration of their position or role within the Company and the risk-based approach.

45. In accordance with paragraph 10 of the AML/CFT Policy, THE COMPANY shall take steps to encourage its potential and existing Counterparties to adopt policies and procedures that are consistent with the principles set in the AML/CFT Policy and these Standards, and to support to the extent possible potential or existing Counterparties in their efforts to prevent, detect, manage, and mitigate ML/FT risks, and to investigate red flags, Suspicious Activities, and suspected ML/FT. To that end, THE COMPANY will provide training and capacity development support or specialized training to such Counterparties in situations:

- (a) Where the potential or existing Counterparty has specifically requested capacity-building support to enable it to effectively prevent, detect, manage, and mitigate ML/FT risks, and to investigate red flags, Suspicious Activities, and suspected ML/FT.
- (b) Where the Executive Director has identified through its accreditation, due diligence, and/or risk assessment processes that such potential or existing Counterparty is lacking sufficient capacity or knowledge to prevent, detect, manage, and mitigate ML/FT, causing potential risk to THE COMPANY project; and
- (c) Where the AML / CFT COMPLIANCE OFFICER has identified through its proactive integrity reviews and other engagements with Accredited Entities that a Counterparty is lacking sufficient capacity or knowledge to prevent and detect risks of ML/FT and other Prohibited Practices, or to receive, handle, or investigate reports of red flags, Suspicious Activities, or suspected ML/FT and other Prohibited Practices.

46. Training and capacity-building support referred in paragraph 45 above should be differentiated according to different needs and capacities of potential or existing Counterparties and may be informed by an AML/CFT capacity assessment. The areas of support and training include but not limited to:

- (a) **Policy Advice:** Support in developing the entity's policies, standards, operating procedures, and governance arrangements with regard to Prohibited Practices including AML/CFT, Whistleblowing and Witness Protection, and investigations;
- (b) **Technical Training:** Know-how in effective ways to implement an AML/CFT compliance program including CDD, risk assessment, and ongoing monitoring; and
- (c) **Experience Sharing:** Providing market information, including data base and system providers to assist entities to enhance their capabilities in assessing and

detecting risks.

XI. Record Retention

47. In accordance with this AML/CFT Policy, THE COMPANY shall ensure mandatory and minimum requirements for record retention for AML/CFT purposes including to demonstrate that due diligence has been undertaken to prevent ML/FT, and to ensure that sufficient information or documentation may be provided when requested by Competent Authorities in any AML/CFT investigation.

48. Guidelines on retaining and retrieving records shall be established to address the following issues:

- (a) The duration and terms of record retention.
- (b) Record storage and internal and external access to records.
- (c) The use of record for investigation purposes.
- (d) Terms of record retention compliance.
- (e) Confidentiality and security of record retention; and
- (f) The scope and contents of records.

XII. Data Protection and Confidentiality

49. Any data, information, and documents, whether in physical or electronic format, obtained during the course of Counterparty Due Diligence ("CDD") or Suspicious Activities monitoring shall be protected and kept confidential in accordance with THE COMPANY policies and procedures and THE COMPANY internal legal framework.

XIII. Right of Interpretation

50. THE COMPANY Executive Director has the ultimate right of interpretation of these Standards. However, for operational purposes, at first instance, the Executive Director delegates this responsibility to AML / CFT COMPLIANCE OFFICER, in consultation with the EAC. Should the Office of the General Counsel ("OGC") have a different opinion on the interpretation of the provisions of these Standards provided by AML / CFT COMPLIANCE OFFICER, OGC shall have the right to present its opinion on the interpretation to the EAC for its decision.

XIV. Authority of the Documents

51. The AML/CFT Standards are a THE COMPANY Executive Director-approved document. Any amendment, enhancement, or update thereto requires the Executive Director's approval.

XV. Review

52. The AML/CFT Standards shall be reviewed biennially or at such intervals as required, to reflect international best practices consistent with evolving FATF recommendations or as otherwise required by the Executive Director or recommended by the AML / CFT COMPLIANCE OFFICER. The reviews shall be conducted by the AML / CFT COMPLIANCE OFFICER in collaboration with THE COMPANY Executive Director.

XVI. Effective Date

53. This Policy shall come into effect following the approval of the Executive Director of THE COMPANY.

Quantum Family-Office, Sofia/BG, April 2023