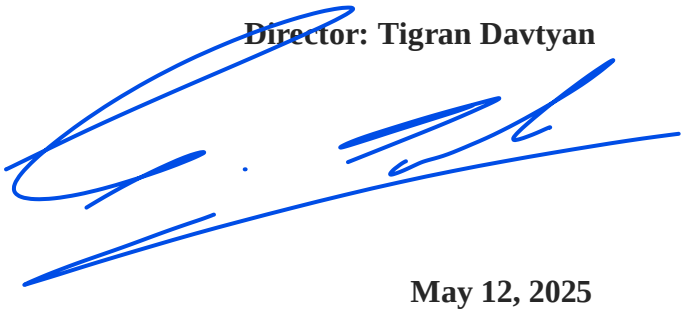
Approved by the resolution N Ո-25-001 of sole partcipant
of "Aktina Capital" limited liability company

Director: Tigran Davtyan



May 12, 2025

"Anti-Money Laundering, Combating the Financing of Terrorism, and Compliance with International Sanctions" Policy

2025

YEREVAN

CONTENT

CHAPTER 1: GENERAL PROVISIONS

1.1. The Anti-Money Laundering and Counter-Terrorism Financing Policy (hereinafter referred to as the "Policy") defines the objectives, tasks, principles, key functions, and implementation approaches of the internal control system of **AKTINA CAPITAL** LLC (hereinafter referred to as the "Company") in the areas of combating money laundering and terrorism financing (hereinafter AML/CTF), combating the financing of the proliferation of weapons of mass destruction (PFWMD), as well as ensuring compliance with international sanctions.

1.2. The AML/CTF Policy has been developed in accordance with the Law of the Republic of Armenia "On Combating Money Laundering and Terrorism Financing" (hereinafter referred to as the "Law"), the regulatory legal acts adopted by the Central Bank of the Republic of Armenia (hereinafter referred to as the "CBA") based on the Law, and the requirements of international treaties of the Republic of Armenia.

1.3. The functions related to the prevention of AML/CTF/PFWMD and the enforcement of international sanctions requirements, as defined by the Law and the regulatory legal acts of the CBA, are carried out within the Company by the Internal Oversight Body (hereinafter referred to as the "IOB"), which operates independently and reports to the General Meeting of the Company's participants (or the sole participant).

1.4. The requirements of this Policy apply to all employees and managers of the Company.

1.5. The objectives of this Policy are to:

1.5.1. Ensure that the Company's activities in the field of AML/CTF/PFWMD are in compliance with the provisions of the Law, as well as the standards and requirements established by international organizations,

1.5.2. Prevent the Company's involvement in AML/CTF/PFWMD-related activities and safeguard the Company's business reputation in both domestic and international business relations,

1.5.3. Ensure that the Company's employees take appropriate actions aimed at identifying suspicious transactions or business relationships related to AML/CTF/PFWMD.

1.5.4. Ensure that the Company's operations comply with international sanctions requirements, and establish the principles and control measures implemented by the Company for the purpose of complying with such sanctions.

1.6. The objective of this Policy is to ensure, in accordance with the requirements of the RA AML legislation, the effective implementation and maintenance of the Company's overall internal control over AML/CTF activities by its employees, as well as to ensure that the Company's risk appetite aligns with the financial sanctions imposed by international organizations.

1.7. The main principles of control for combating AML/CTF are:

1.7.1. Within the scope of their functions and regardless of their position, the participation of all Company employees in the implementation of internal controls aimed at combating AML/CTF/PFWMD,

1.7.2. For the purpose of combating AML/CTF/PFWMD and in compliance with the requirements of the Law, the individual accountability of all Company employees in the implementation of internal controls, as well as the confidentiality of the information obtained during the execution of the mentioned operations (functions),

1.7.3. In the course of implementing internal controls aimed at combating AML/CTF/PFWMD, the Company shall not disclose to its clients or any other persons any information regarding the measures undertaken by the Company,

1.7.4. Establishment of rules and methods for internal control aimed at combating AML/CTF/PFWMD,

1.7.5. Application of a unified approach to internal control for combating AML/CTF/PFWMD, ensuring its implementation through the regulation of employee actions during the execution of individual business processes.

1.8. The main principles of control for ensuring compliance with international sanctions are:

1.8.1. the participation of all Company employees in ensuring compliance with international sanctions, regardless of their position or scope of responsibilities,

1.8.2. establishment of rules and methods for ensuring compliance with international sanctions,

1.8.3. Application of a unified approach to international sanctions, as well as regulation of employee actions during the execution of individual business processes to ensure compliance,

1.8.4. implementation of training and awareness programs on international sanctions to enhance employees' knowledge and understanding,

1.8.5. conducting periodic monitoring and evaluation to ensure the effectiveness of the implemented measures.

1.9. The key terms used in this Policy correspond to those defined in the Law, unless otherwise specified.

CHAPTER 2: PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING WITHIN THE COMPANY

2.1. Minimum Requirements for the Company's Participants and Executive Body

2.1.1. The Company's AML and international sanctions risk management system is based on the Three Lines of Defense model. Under this model, the first line of defense for AML and sanctions-related controls is assigned to the employees of the customer service unit (hereinafter also referred to as "Responsible Employees"); the second line of defense functions are carried out by the Internal Oversight Body (IOB); and the third line of defense is ensured by Internal Audit.

2.1.2. The General Meeting of the Company's Participants (or the sole participant) is responsible for establishing an effective internal system for combating AML/CTF/PFWMD and ensuring compliance with international sanctions. It also ensures the ongoing operation and oversight of this system.

2.1.3. In the area of AML/CTF/PFWMD and ensuring compliance with international sanctions, the General Meeting of the Company's Participants (or the sole participant) performs the following key functions:

2.1.3.1. Approves the Company's internal legal acts related to AML/CTF and international sanctions compliance, including the annual work plan of the Internal Oversight Body (IOB);

2.1.3.2. Oversees the implementation of necessary measures for identifying, assessing, and reviewing risks in the AML/CTF and international sanctions compliance domain, as regularly reviewed by the IOB;

2.1.3.3. Oversees the implementation of internal measures by the Company's executive body aimed at ensuring AML/CTF and international sanctions complianc;

2.1.3.4. Reviews and approves measures aimed at eliminating deficiencies identified during audits or other inspections (reviews) in the area of AML/CTF and international sanctions compliance, provides instructions for addressing those deficiencies, and monitors the implementation process;

2.1.3.5. Receives, reviews, and approves reports submitted by the Internal Oversight Body (IOB) at least on a semiannual basis;

2.1.3.6. Grants approval for the appointment of an IOB employee by the executive body;

2.1.3.7. Performs other functions as defined by the Law, this Policy, and other legal acts adopted pursuant to the Law:

2.1.4. The executive body of the Company shall perform the following key functions in the field of anti-money laundering (AML), counter-terrorism financing (CTF), and compliance with international sanctions:

2.1.4.1. Ensures the implementation of the AML/CTF and international sanctions compliance strategy and policy as approved by the meeting of the Company's participants;

2.1.4.2. Ensures the implementation and operation of internal processes for identifying, assessing, examining, and monitoring AML/CTF and international sanctions compliance risks;

2.1.4.3. Ensures the full and effective implementation of legal acts adopted under the Law and this Policy, and supervises compliance with them;

2.1.4.4. Ensures adequate training of the Company's employees in the field of AML/CTF and international sanctions compliance;

2.1.4.5. Is responsible for implementing the AML/CTF and international sanctions compliance policy and processes approved by the participants' meeting, as well as for ensuring their ongoing effective operation;

2.1.4.6. Implements measures to eliminate deficiencies identified during studies conducted by the Internal Oversight Body (IOB), including audits or other inspections;

2.1.4.7. Ensures the Internal Oversight Body is provided with the necessary logistical and material resources;

2.1.4.8. Performs other functions as defined by the Law, this Policy, and other legal acts regulating the AML/CTF field.

2.2. Duties, Powers, and Requirements of the Internal Oversight Body (IOB)

2.2.1. The work of the Internal Oversight Body (IOB) within the Company is aimed at the prevention of money laundering and terrorism financing (ML/TF), as well as the establishment of effective processes to ensure compliance with international sanctions, including:

2.2.1.1. Implementation of mechanisms for customer identification, due diligence, and data updating, as well as conducting ongoing monitoring, transaction reviews, and checks;

2.2.1.2. Introduction and application of a risk-based system for combating ML/TF;

2.2.1.3. Submission of information and reports as required by the legislation of the Republic of Armenia;

2.2.1.4. Organization of record-keeping for information and documents necessary for the arrangement of AML activities;

2.2.1.5. Organization of staff training aimed at enhancing the effectiveness of AML measures and compliance with international sanctions;

2.2.1.6. Implementation and supervision of the Company's processes for ensuring compliance with international sanctions.

2.2.2. The implementation of the AML/CFT system within the Company (including the development and revision of internal legal acts and their submission for approval to the Company's General Meeting of Participants (or sole participant) and the Executive Body) and the oversight thereof shall be carried out by the Internal Oversight Body (IOB), which in its operations is guided by the legislation of the Republic of Armenia, international standards and requirements, the Charter of the Company, this Policy, the Company's internal legal acts, the decisions and directives of the General Meeting of Participants (or sole participant), and the orders and instructions of the Executive Body.

2.2.3. The head and employees of the IOB, when performing the functions defined by this Policy and internal legal acts adopted based on it, act independently and hold a senior management status.

2.2.4. The head and employees of the IOB have the right to directly report any issues arising in the area of AML/CFT and compliance with international sanctions to the Company's General Meeting of Participants (or sole participant), and to participate in the discussions of such matters held by the General Meeting of Participants (or sole participant) and the Executive Body.

2.2.5. The head and employees of the IOB shall have direct and immediate access to all information acquired and maintained by the Company as required by Armenian legislation and this Policy, including all documents related to customer accounts and executed transactions.

2.2.6. The head and employees of the IOB have the right to request clarifications from any employee of the Company regarding transactions or business relationships, as well as concerning customers, authorized persons, and beneficial owners.

2.2.7. The Internal Oversight Body (IOB):

2.2.7.1. Assesses the risk associated with the customer and the transaction or business relationship;

2.2.7.2. Conducts analyses for the purpose of identifying suspicious transactions or business relationships and retains the results of such analyses;

2.2.7.3. Makes final decisions regarding the classification of transactions or business relationships as suspicious, their suspension, rejection, or termination, as well as the freezing of assets of persons associated with terrorism or the proliferation of weapons of mass destruction;

2.2.7.4. Ensures submission of reports on transactions subject to mandatory reporting, suspicious transactions or business relationships to the Central Bank of Armenia on behalf of the Company;

2.2.7.5. Provides consultancy and support to the General Meeting of Participants (or sole participant) and the Executive Body in fulfilling their functions related to AML/CFT and compliance with international sanctions;

2.2.7.6. Conducts training for the Company's employees in the fields of AML/CFT and international sanctions (including relevant legislation, internal legal acts of the Company, and practical examples);

2.2.7.7. Conducts AML risk assessments in cases where new products, new methods of offering existing products, financial instruments, or processes are introduced or significantly changed. Such risk assessments must be performed prior to the launch of the new services, methods, or the application of new or emerging technologies.

2.2.7.8. At least semi-annually, reviews the compliance of executed transactions, established business relationships, and employee conduct with the Law, this Policy, and the Company's internal legal acts adopted on the basis thereof. The IOB presents reports on the results of such reviews, as well

as on other matters raised by the Central Bank of Armenia, to the Executive Body and the General Meeting of Participants (or sole participant).

2.2.8. The Internal Oversight Body (IOB) makes final decisions regarding the classification of a transaction or business relationship as suspicious, its suspension, rejection, or termination, as well as the freezing of assets of persons associated with terrorism. It also ensures the submission of reports to the Central Bank of Armenia (CBA) as required by the Law and this Policy and performs other functions defined by the Company's internal legal acts.

2.2.9. Following the submission of a report on a suspicious transaction or business relationship to the CBA, the IOB informs the Executive Body and the General Meeting of Participants (or sole participant) about its decision to classify the transaction or business relationship as suspicious, suspend it, or freeze assets related to persons associated with terrorism.

2.2.10. The prevention of ML/TF is the responsibility of every employee of the Company. All employees are required to immediately inform the IOB of any suspicious transaction related to a customer, agent, authorized person, or any other third party involved in a business relationship.

2.2.11. Instructions, directives, and orders issued by the Head of the IOB concerning ML/TF prevention are mandatory for all employees of the Company. Information relating to such instructions must be retained for at least five (5) years, unless a longer retention period is established by the Company's internal legal acts.

2.2.12. The Head of the Internal Oversight Body (IOB) may be appointed a person who meets both the minimum criteria established by the Regulation "On the Minimum Requirements for Reporting Entities in the Field of Anti-Money Laundering and Counter-Terrorist Financing," approved by Decision No. 279-N of the Central Bank of Armenia dated October 7, 2014, and the following additional requirements:

- 2.2.12.1. Holds a higher education degree and a professional qualification certificate (in the financial sector) recognized internationally,
- 2.2.12.2. Has at least 1 (one) year of work experience in the field of AML/CTF, or at least 5 (five) years of managerial experience related to banking/investment operations.,
- 2.2.12.3. Has knowledge of the legislation and other regulatory legal acts of the Republic of Armenia related to AML/CTF, international standards in the field, and internal control procedures.
- 2.2.12.4. Has knowledge of FATF Recommendations and principles presented by international organizations related to AML/CTF risk assessment; international qualification is considered an advantage.
- 2.2.12.5. Communicates fluently in Armenian and Russian and has a good command of English.

CHAPTER 3. RISK-BASED APPROACH AND RISK MANAGEMENT

3.1. In order to provide a comprehensive overview of the ML/TF risk management system within the Company, this Policy outlines the key principles for mitigating ML/TF risks and defines the Company's risk appetite concerning anti-money laundering, counter-terrorism financing, and sanctions compliance (see Annex 1). Detailed processes, tools, and related matters of ML/TF risk management are described in other internal legal acts of the Company (AML/CFT Procedure).

3.2. The assessment of potential and existing ML/TF risks is conducted based on the evaluation of the Company's inherent ML/TF risks and the effectiveness of its internal control systems. As a result, the Company identifies its residual ML/TF risk in order to distinguish between acceptable and unacceptable risks and to implement

an adequate risk management framework. Potential and existing ML/TF risks are reviewed at least once a year.

3.3. The Company determines the ML/TF risk level for each client. Employees of the Company perform monitoring, detection, assessment, and analytical examination of the risk level, as well as implement mitigation and prevention measures for ML/TF risks.

3.4. The client's ML/TF risk level is assessed by employees of the Company based on the analysis of available information and documents regarding the client, their activities, and any transactions conducted by the client.

3.5. For effective risk management, during the customer due diligence process, ML/TF risk is assessed as high, medium, or low. The following components form the basis for such assessment:

3.5.1. Country or geographical area risk,

3.5.2. Transaction or business relationship risk,

3.5.3. Product, service, or delivery method risk.

3.6. Enhanced due diligence is applied to high-risk clients, standard due diligence to medium-risk clients, and simplified due diligence may be applied to low-risk clients.

3.7. Simplified due diligence shall not be applied in cases where the transaction or business relationship is deemed suspicious or where a high ML/TF risk criterion is present, except in cases where a medium or high-risk criterion exists, but the transaction qualifies as low-risk and does not exceed the equivalent of one thousand times the minimum wage.

3.8. If a new risk criterion arises during the course of the business relationship with a client, the responsible employee must inform the Compliance Unit (CU) and obtain its opinion on whether to revise the risk level and apply appropriate due diligence measures in accordance with the newly determined risk level.

3.9. The Company continuously aims to reduce the number of high-risk clients based on the outcomes of their due diligence. The Company's risk appetite for ML/TF/Proliferation Financing (PF) is defined by a maximum threshold (percentage) for high-risk clients.

4. CHAPTER 4: MINIMUM REQUIREMENTS FOR CUSTOMER AND TRANSACTION DUE DILIGENCE

4.1. The Company may establish a business relationship with a customer only after obtaining the information required for customer identification as stipulated by this Policy and other internal legal acts of the Company, and after verifying the customer's identity, including through identification by means of audiovisual telecommunication tools. The Company may verify the customer's identity based on the information required for identification during or after the establishment of the business relationship within a reasonable period, but not exceeding seven (7) days, provided that the risk is effectively managed and that this is necessary to avoid disruption of normal business relations with the customer.

4.2. The Company shall not establish or continue business relations with foreign individuals who, lacking any economic and/or personal interest in the Republic of Armenia, fail to provide reasonable information substantiating economic or other lawful grounds for servicing financial flows through the Armenian financial system.

4.3. The Company shall commence customer due diligence from the moment the customer applies to the Company for establishing a business relationship and shall continue it until the contractual relationship between the customer and the Company is terminated.

4.4. Customer due diligence includes collecting, analyzing, and assessing information about the customer based on the data available to the Company.
4.5. The Company may establish a business relationship with a customer only after receiving the information (including documents) required for customer identification and verifying the customer's identity.
4.6. The Company must ascertain whether the customer is acting on their own behalf or on behalf of or for the benefit of another person and take measures to identify and disclose the customer's beneficial owner.
4.7. Enhanced due diligence on customers shall be conducted at a minimum in the following cases:
    4.7.1. Upon establishing a business relationship with the customer, the beneficial owner, or an authorized person of the customer;
    4.7.2. When doubts arise regarding the authenticity or completeness of previously obtained information related to the customer's identification (including documents);
    4.7.3. When suspicions arise from the perspective of money laundering and terrorist financing (ML/TF).
4.8. In cases where the customer's risk level factors are low, the Company shall conduct simplified due diligence on the customer's transactions and business relationships.
4.9. Simplified due diligence on the customer's transactions cannot be conducted if any suspicion indicators exist in the customer's transactions or business relationships.
4.10. If the customer's risk is neither high nor low, the risk classification shall be considered medium.
4.11. In the presence of customers with a medium risk level, the Company shall continuously conduct appropriate due diligence of the transactions and business relationships of such medium-risk customers.
4.12. In the presence of high-risk factors, the Company shall conduct enhanced due diligence on the customer's transactions and business relationships. Enhanced due diligence shall also be performed if a high-risk indicator is identified or arises during a transaction or business relationship.
4.13. High-risk indicators, in addition to those established by the legislation of the Republic of Armenia, are described in other internal legal acts of the Company and in Appendix 1 attached to this Policy.
4.14. Information regarding the customer and the transactions carried out by the customer (including information about beneficial owners) shall be updated with the following frequency:
    4.14.1. Low risk — every 2 years;
    4.14.2. Medium risk — annually;
    4.14.3. High risk — every 6 months;
    4.14.4. Politically exposed persons (PEPs) — every 3 months.
4.15. A politically exposed person (PEP) is an individual holding or having held prominent public, political, or governmental functions, as well as persons holding significant functions in international organizations (including family members or closely related persons). The scope of politically exposed persons does not include individuals holding middle or low-level functions.
4.16. To determine whether an individual is politically exposed, the Company may conduct reviews of publicly available information sources and private databases concerning politically exposed persons.

5. CHAPTER 5. CLASSIFICATION OF A TRANSACTION OR BUSINESS RELATIONSHIP AS SUSPICIOUS, THEIR SUSPENSION, REJECTION OR TERMINATION, AND FREEZING OF ASSETS RELATED TO TERRORISM

5.1. A transaction may be classified as suspicious either at the time of its execution (while servicing the client) or during the ongoing due diligence process, including monitoring of client transactions.

5.2. A transaction or business relationship, including an attempt to execute a transaction or establish a business relationship, shall be classified as suspicious and a suspicious transaction or business relationship report shall be submitted to the Central Bank of Armenia if there is suspicion or reasonable grounds to suspect that the property involved in the transaction or business relationship was obtained through criminal means, is related to terrorism, terrorist acts, terrorist organizations or individual terrorists, or persons financing terrorism, or has been used, or there is an intention to use it, for the purpose of terrorism or by terrorist organizations, individual terrorists, or persons financing terrorism.

5.3. The issue of classifying a transaction or business relationship as suspicious and submitting a suspicious transaction or business relationship report to the Central Bank of Armenia shall be considered in the following cases:

5.3.1. when the situation under consideration fully or partially corresponds to the criteria or typologies of a suspicious transaction or business relationship; or

5.3.2. when it becomes apparent that although the suspicious nature of the concluded or proposed transaction or business relationship does not derive directly from the criteria or typologies of suspicious transactions or business relationships, the logic of its execution, its flow (dynamics), or other circumstances give reason to assume that it may be carried out for the purpose of money laundering and/or terrorism financing.

5.4. In cases where, as a result of the review, the transaction or business relationship is not classified as suspicious and a report on a suspicious transaction or business relationship is not submitted to the Central Bank of Armenia, the justification for not classifying the transaction or business relationship as suspicious, the conclusions drawn, the analysis process, and its outcomes shall be documented and retained by the Company for at least 5 years, unless a longer period is prescribed by the Company's internal legal acts.

5.5. The Compliance Officer has the right to suspend a transaction or business relationship for up to 5 days, and in the case of receiving an instruction from the Central Bank of Armenia, is obliged to suspend it for 5 days and immediately submit a report on the suspicious transaction or business relationship to the Central Bank of Armenia.

5.6. A decision by the Central Bank of Armenia to suspend a transaction or business relationship shall be executed immediately upon receipt by the Company.

5.7. A decision by the Company or the Central Bank of Armenia to suspend a transaction or business relationship may be declared void prior to the expiration of the suspension period only by the Central Bank of Armenia, either on its own initiative or upon the Company's request, if further suspension is deemed unnecessary.

5.8. If no decision is received from the Central Bank of Armenia regarding the extension of the suspension, the suspension shall be considered null and void.

5.9. Until the receipt of information on the lifting of the suspension, the Responsible Employee shall not proceed with the execution of the respective transaction.

5.10. The refusal to execute a transaction or to establish a business relationship shall take place in the following cases:

5.10.1. upon receipt of the relevant instruction defined by the decision of the Central Bank of Armenia,

5.10.2. in case of the impossibility of conducting proper due diligence (CDD),

5.10.3. in cases where the persons are subject to sanctions; in such cases, clients' transactions are carried out in accordance with the requirements of international sanctions, and in the presence of a risk of breaching those requirements, such transactions shall be rejected.

5.11. Termination of a transaction or a business relationship shall be executed in the following cases:

5.11.1. in case of the impossibility or failure of ongoing proper due diligence of the Company's client.

5.12. In cases of refusal to execute a transaction or to establish a business relationship, or of termination thereof, the matter of classifying them as suspicious shall be considered.

5.13. It is prohibited to make property, economic resources, or financial or other related services available, directly or indirectly, in whole or jointly, to persons related to terrorism or for their benefit.

5.14. Property that is directly or indirectly owned or controlled by persons included in the United Nations Security Council resolutions, in accordance with them, or listed by the Central Bank of Armenia as being related to terrorism or the proliferation of weapons of mass destruction shall be subject to immediate freezing without prior notice to the persons concerned. Lists of persons related to terrorism are published by the Central Bank of Armenia on its official website.

5.15. In case of obtaining information indicating that a person falls within the definition of a person related to terrorism or the proliferation of weapons of mass destruction, the Company is obliged to immediately report this to the Central Bank of Armenia.

5.16. In case of freezing property belonging to persons related to terrorism or the proliferation of weapons of mass destruction, the transaction or business relationship shall immediately be classified as suspicious and a report on the suspicious transaction or business relationship shall be submitted to the Central Bank of Armenia.

5.17. All employees of the Company, regardless of their position, are prohibited from disclosing or making known to any person the fact that a report or other information has been submitted to the Central Bank of Armenia concerning a client and/or transaction, including the classification, suspension, or freezing of a transaction or business relationship, or the inclusion of the client in a "Blacklist".

6. CHAPTER 6. EMPLOYEE TRAINING

6.1. Training on anti-money laundering and combating the financing of terrorism (AML/CFT), as well as compliance with international sanctions, shall be organized by the Company for its employees, including the General Meeting of Participants (or sole participant), the executive body, and the Internal Audit function at least once a year. For newly hired employees, the training must be conducted within three (3) months from the commencement of their employment. To assess the effectiveness of training, questions related to AML/CFT and compliance with international sanctions shall be included in the qualification examinations (certification tests) for both new and existing employees.

6.2. The Compliance Officer (CO) shall develop and annually update the Company's training program for employees. The training program shall mandatorily include changes in Armenian legislation in the AML/CFT field, regulatory requirements for compliance with international sanctions, the internal regulatory framework implemented by the Company in this regard, any changes thereto, and the training schedule. The training program shall be presented for approval to the General Meeting of Participants (or the sole participant) as part of the CO's annual plan.

6.3. The CO may also organize specific thematic trainings, testing sessions, and discussions.

6.4. Training materials, information about the participating employees, and supporting documentation confirming attendance shall be recorded and retained for at least five (5) years, unless a longer period is prescribed by the Company's internal legal acts.

7. CHAPTER 7. PRINCIPLES AND PROCEDURE FOR COMPLIANCE WITH INTERNATIONAL SANCTIONS

7.1. International sanctions (hereinafter referred to as the "Sanctions") are imposed through international legal instruments adopted by international and intergovernmental organizations, international treaties concluded between countries, as well as laws and other legal acts adopted by governmental authorities of various countries, which are regularly monitored by the AML Compliance Officer.

7.2. When servicing clients, the relevant units of the Company undertake measures to comply with the sanctions imposed by the United Nations, the United States, the European Union, the United Kingdom, and, when necessary, also by other countries, their governmental authorities, international organizations, and intergovernmental institutions.

7.3. The Company complies with the following types of Sanctions:

7.3.1. Restrictions imposed on specific countries;

7.3.2. Restrictions imposed on specific goods and/or sectors of activity of certain countries or territories;

7.3.3. Restrictions imposed on specific individuals or entities;

7.3.4. Requirements related to asset freezing.

7.4. The Company's management ensures the implementation of necessary measures to comply with the international restrictions and Sanctions requirements defined under this Policy.

7.5. The employees of the Company shall service clients in accordance with the approach adopted by the Company regarding restrictions imposed on countries, goods originating from certain countries or regions, and/or sectors of activity.

7.6. The executive body ensures the implementation and monitoring of international restrictions and Sanctions requirements within the Company, as well as the training and awareness of the staff.

7.7. The Company ensures compliance with Sanctions requirements in its dealings with clients, partners, service providers, including partner financial institutions, companies providing custodial services, suppliers, and all types of third parties.

7.8. In case of ambiguities regarding the interpretation of the requirements set forth by the Sanctions, the application of the relevant provisions shall be interpreted by the Head of the AML Compliance Officer, with the support of the Company's legal and compliance functions, where necessary.

7.9. Based on the approach of partner financial institutions, potential risks arising from Sanctions, and commonly accepted practices in the business environment, the AML Compliance Officer may recommend the application of stricter measures than those prescribed by Sanctions if deemed necessary to mitigate reputational and financial risks.

7.10. The coordination of compliance with and implementation of international Sanctions requirements, staff training when necessary, and the implementation of tools and processes for managing related issues within the Company shall be performed by the AML Compliance Officer.

7.11. Regardless of position, all employees of the Company are prohibited from assisting, remaining inactive, concealing or disguising information, or providing advice to clients for the purpose of evading Sanctions requirements.

7.12. To verify matches against individuals subject to Sanctions or listed by the competent authorities, the Company uses a dedicated information database.

7.13. Any non-compliance with Sanctions-related requirements, as well as inquiries or requests from third parties, must be reported to the AML Compliance Officer immediately.

7.14. The AML Compliance Officer assists in preparing responses to inquiries received from Sanctions supervisory authorities and partner financial institutions, specifically regarding questions related to the observance of Sanctions.

7.15. In cases where a legal entity is 50 (fifty) percent or more owned, directly or indirectly, by an individual and/or legal entity subject to Sanctions, such legal entity shall also be considered as subject to Sanctions. The AML Compliance Officer may apply a stricter approach, including enhanced due diligence, considering

the requirements of legislation, business practices, risks arising from the intended transaction or business relationship, approaches of international partners, and also in cases where the information about all beneficial owners of the legal entity is not exhaustive or there are doubts regarding the true beneficial owner.

7.16. When establishing a business relationship or entering into transactions with persons included in Sanctions lists, the Company shall be guided by the requirements arising from the Sanctions, the relevant legal act establishing the Sanction, and the relevant interpretations or clarifications thereof.

7.17. In the case of transactions involving entities that are under Sanctions and/or included in relevant official lists, or entities connected to such persons, the final decision on proceeding with the transaction shall be made following a discussion initiated by the Head of the AML Compliance Officer with the participation of the executive body and, where necessary, other relevant persons designated by the executive body. The discussion and final decision must be properly documented.

7.18. The Company's review of transactions in the context of international restrictions and Sanctions shall include, at a minimum, the collection and analysis of the following data:

7.18.1. Identification and assessment of the client's residency from the perspective of international Sanctions,

7.18.2. Determination and assessment of the foreign client's center of vital interests from the perspective of international Sanctions,

7.18.3. Review of other third parties, partners, involved countries, currencies, source of funds, purpose, nature of goods and services, activities and economic purpose, and other factors such as citizenship, place of birth, residence, etc., which, in the opinion of the AML Compliance Officer or the executing financial institution, may play a material role in Sanctions evasion.

7.19. Prior to establishing a partnership, the Company, as part of its due diligence process, shall assess, among other things, the potential partner entity's approach and policy on compliance with Sanctions requirements, based on a risk-based approach and adherence to the provisions of relevant Sanctions-related legal acts.

7.20. If at any time an existing client or their transactions become subject to Sanctions, the Company shall, within a reasonable period, apply the relevant Sanctions requirements, which may include terminating the business relationship and/or rejecting transactions, in accordance with applicable legal requirements. These provisions shall also apply to the Company's relations with partner financial institutions, suppliers, and other cooperating parties.

7.21. In the case of a transaction or business relationship characterized by high Sanctions violation risk indicators, the Company may decide to reject the transaction, refuse to establish a business relationship, or terminate an existing relationship. The final decision shall be made through a discussion initiated by the AML Compliance Officer with the participation of the executive body and, where necessary, other relevant persons designated by it. The results of the discussion and the final decision must be documented.

8. CHAPTER 8. OTHER PROVISIONS

8.1. This Policy is subject to revision in the event of changes to the legislation of the Republic of Armenia, standards and requirements related to anti-money laundering and combating the financing of terrorism (AML/CFT), as well as in other necessary circumstances.

8.2. All employees of the Company, including management, are required to familiarize themselves with this Policy.

Annex 1
Cases of Refusal to Establish Business Relationships,
Qualitative Criteria Characterized by High-Risk Indicators or Special Service

Table 1

	Description	***Risk appetite***	***Comment***
1.	Accounts under anonymous or fictitious names, or accounts expressed solely through numerical, alphabetical, or other symbolic codes.	Forbidden	-
2.	Any type of business relationship with shell banks or financial institutions servicing shell banks.	Forbidden	-
3.	Transactions in securities conducted on a bearer basis.	Forbidden	-
4.	Persons registered in or operating from jurisdictions listed on the FATF Public Statement ("blacklist")[1]:	Forbidden	-
5.	Persons included in the sanctions lists of the UN, US, EU, and UK.	Forbidden	-
6.	Legal entities whose shareholders owning 50% or more of shares are listed in the sanctions lists of OFAC [2], EU, or UK.	Forbidden	-
7.	Individuals and legal entities identified in publicly available credible sources or widely used screening databases (e.g., Worldcheck, Accuity, etc.) as "sanction-associated persons," including:	Forbidden	-

[1] https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html
[2] *U.S. Treasury Office of Foreign Assets Control (OFAC)*

	• Persons directly connected to individuals or entities listed in sanctions lists, such as family members (spouse, children, parents), and in the case of legal entities – owners, beneficial owners, or senior management members.[3]		
8.	Individuals and legal entities involved in ML/TF or PF-related criminal activities.	Forbidden	Including as a suspect.
9.	Individuals and legal entities, including non-commercial organizations, registered, resident, or operating in jurisdictions identified as high-risk for ML/TF or PF purposes.[4]	Forbidden/Limited	Business relationships may be established when the economic or other lawful purposes are evident, for example, due to the presence of the Armenian community in certain countries, among other reasons.
10.	Persons registered in, residents of, or operating in countries characterized by high corruption risks, particularly in high-risk sectors such as construction, pharmaceuticals, mining, and other similar industries.[5]	Limited/ High risk	A business relationship may be established provided that, in addition to the complete collection of information required by law and the Company's internal legal acts for AML measures (and, if necessary, enhanced AML measures), the account-opening company has and applies the necessary procedures and is characterized as a reputable organization. Furthermore, there must be reasonable grounds to believe that the economic and other lawful motives for using the financial system of the Republic of Armenia are present.

[3] *Board/management/executive body members*

[4] *The list of countries is determined based on the jurisdictions identified by the Competent Authority within the scope of Armenia's National ML/TF Risk Assessment for 2021–2023. In particular, it includes countries that are either in a state of war or known to be locations of active operations by terrorist groups (e.g., Afghanistan, Jordan, Lebanon, Türkiye, Iraq, Pakistan, Syria, Libya, Yemen, Bangladesh).At the same time, this list is not exhaustive, and other countries or territories may also be considered high-risk based on prevailing geopolitical developments and other relevant circumstances at the time of assessment.*

[5] *The list of countries characterized by high corruption risks is defined based on the Corruption Perceptions Index 2024, published by Transparency International (https://images.transparencycdn.org/images/Report-CPI-2024-English.pdf)☐).*
Countries that received a score below 40 on the respective scale are considered high-risk from a corruption perspective.

11.	Politically Exposed Persons (PEPs), their associates, and family members from countries with high corruption risks.[6]	Forbidden/ Limited	Exceptions apply in cases where, in addition to the complete collection of information required by law and the Company's internal legal acts for AML (and enhanced AML) purposes, the source of income is clearly substantiated, the individual's income is consistent with their assets and the volume of intended transactions, and no negative information is found in publicly accessible sources or private information databases regarding the individual, their related persons, or family members. Furthermore, there are reasonable grounds to believe in the economic and other lawful motives for using the financial system of the Republic of Armenia.
12.	Trusts and similar legal arrangements, as well as complex legal structures registered, resident, or operating in jurisdictions with ineffective transparency and information exchange frameworks.[7]	Forbidden	-
13.	Organizers of casinos, gambling (including online gambling), and lotteries operating from countries with strategic AML/CFT deficiencies or those rated as having "Low" effectiveness in supervising such sectors according to mutual evaluation reports.	Forbidden	-
14.	Entities conducting activities subject to licensing under applicable law but operating without a license in countries where such licensing is mandatory.	Forbidden	-
15.	Entities engaged in the trade of arms and weapons.	Forbidden	Except for the Ministry of Defense of the Republic of Armenia.

[6] *Refer to the previous footnote.*

[7] *Countries with ineffective regimes in terms of information exchange and transparency may include those jurisdictions that, based on evaluations by the FATF and FATF-style regional bodies, have received a "Low" effectiveness rating for both Immediate Outcome 2 (International Cooperation) and Immediate Outcome 5 (Legal Persons and Arrangements). Legal entities and arrangements, including trusts, that are registered or operate in such countries may be considered high-risk. The relevant list of countries is provided as of March 2025. (https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html).*

16.	Clients involved in the production or trade of dual-use goods and/or goods with environmentally hazardous impact.	Forbidden	-
17.	Individuals and entities investing in crypto-assets.	Limited	An exception is made for contracts for difference (CFDs), where the client does not actually own the underlying assets.
18.	Embassies, consulates, and similar diplomatic representations.	High risk	
19.	Non-commercial organizations, except for those associated with countries classified as high-risk from an AML/CFT perspective.	High risk	
20.	Entities engaged in the mining industry.	High risk /Limited/Forbidden	There is an international coalition regarding transparency in the extractive industries sector — the Extractive Industries Transparency Initiative (EITI). Resident organizations of member countries may be classified as High Risk, while those from non-member countries may be classified as Limited or Forbidden, depending on the presence of other risk factors.
21.	Companies involved in the extraction and processing of precious stones and metals.	High risk	
22.	Entities characterized by extensive use of cash (including restaurants, retail shops, liquor stores, tobacco suppliers, etc.), excluding those related to countries with strategic AML/CFT deficiencies.	High risk	
23.	High Net Worth Individuals (HNWIs) with at least USD 1 million in highly liquid assets, cash, or bank account balances.	High risk	

24.	Trusts and similar legal arrangements, as well as complex legal entities, excluding those registered or operating in prohibited jurisdictions.	High risk	
25.	Clients whose servicing, in the well-founded opinion of the Company's AML Officer and/or based on alerts received from the Competent Authority, poses reputational or other material risks, regardless of the risk appetite defined in this document.	High risk/ Limited/ Forbidden	

Table 2

Quantitative Risk Appetite Criteria and Special Rules for Transaction Execution

	Description	**Risk appetite**	**Deviations Approved by the Highest Management Body**	**Comment**
1.	Proportion of non-resident clients in the overall client base	70%	5%	Conduct data updates and risk reassessments once annually.
2.	Number of high-risk clients in the overall client base	20%	5%	Conduct data updates and risk reassessments every 6 (six) months.
	Including within the high-risk category:			
3.	Proportion of high-risk individual clients	55%	3%	Perform data updates and risk reassessments every six months
3.1.	Proportion of politically exposed persons (PEPs) / high-net-worth clients among high-risk individual clients	70%	3%	
4.	Proportion of high-risk legal entities	45%	3%	
4.1.	Proportion of high-risk financial institutions among high-risk legal entities	35%	1%	
5.	Companies with shareholders included in the sanction lists of FATF, EU, and the UK, whose total shareholding does not exceed 50%.	1%	1%	On the condition that the company is capable of performing Customer Due Diligence (CDD) with respect to the transactions of the relevant customers