Approved by
by the Sole Participant of
"WILCO" LLC
PARADEPLATZ LIMITED
Stella Makri,
for and on behalf of Alsteris Management Limited
April 2025

(signature)

ANTI-MONEY LAUNDERING, COMBATTING TERRORISM FINANCING AND INTERNATIONAL SANCTIONS COMPLIANCE POLICY

2025
Yerevan

WILCO

TABLE OF CONTENTS

CHAPTER 1. GENERAL PROVISIONS

1.1. The Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter referred to as the "Policy") defines the objectives, tasks, principles, main functions, and implementation approaches of the internal control system in the areas of combating money laundering and terrorist financing (hereinafter AML/CTF), financing of the proliferation of weapons of mass destruction (PF), as well as ensuring compliance with international sanctions at “WILCO” LLC investment company (hereinafter the "Company").

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

1.3. The functions related to the prevention of AML/CTF/PF and ensuring compliance with international sanctions, as defined by the Law and normative legal acts of the CBA, are implemented within the Company by the Internal Monitoring Unit (hereinafter the "IMU"), which operates independently and reports to the sole participant of the Company.

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:

- Align the Company's activities in the field of AML/CTF/PF prevention with the provisions of the Law, as well as the standards and requirements published by international organizations,
- Exclude the Company's involvement in ML/TF/PF transactions, and preserve the Company's business reputation in both domestic and international business relations,
- Ensure the implementation of actions by Company employees aimed at identifying suspicious transactions or business relationships related to ML/TF/PF,
- Ensure that operations carried out by the Company comply with the requirements of international sanctions, including the definition of the principles and control measures applied by the Company for this purpose.

1.6. The aim of this Policy is to implement and maintain overall internal control by the Company's personnel in accordance with the RA legislation on combating ML/TF, and to ensure compliance with financial sanctions established by international organizations in accordance with the Company's risk appetite.

1.7. The key principles of control for the purposes of combating ML/TF are:

- Participation of all employees of the Company in the implementation of internal control measures for combating ML/TF/PF, regardless of their functions and position,
- Individual responsibility of all employees in implementing internal control in accordance with the Law, maintaining the confidentiality of the information received for that purpose,
- Prohibition on informing the Company's clients or other persons about the measures undertaken by the Company as part of internal control for ML/TF/PF purposes,
- Establishment of internal control rules and methods aimed at combating ML/TF/PF,
- Application of a unified approach to internal control and regulation of employee actions during the execution of specific business processes to ensure its implementation.

1.8. The key principles of control for the purpose of complying with international sanctions are:

- Participation of all Company employees in the process of ensuring compliance with international sanctions, regardless of their functions and position,
- Establishment of rules and methods for ensuring compliance with international sanctions,
- Application of a unified approach to international sanctions compliance and regulation of employee actions during the execution of specific business processes,

- Implementation of training and awareness-raising programs on international sanctions to enhance employee knowledge,
- Conducting regular monitoring and assessment to ensure the effectiveness of the measures.

1.9. The main concepts used in this Policy correspond to those defined in the Law.

CHAPTER 2. MINIMUM REQUIREMENTS PRESENTED TO THE SOLE PARTICIPANT OF THE COMPANY AND TO THE EXECUTIVE BODY

2.1. The ML/TF and international sanctions risk management system within the Company is based on the three lines of defense model, where the first line of defense functions related to AML/CFT and international sanctions compliance are performed by Responsible Employees[1], the second line by the Internal Monitoring Unit (IMU), and the third line by Internal Audit.

2.2. The Sole Participant of the Company is responsible for establishing an effective internal system to ensure AML/CFT/PF compliance and compliance with international sanctions and for overseeing its ongoing operation and control.

2.3. In the field of AML/CFT/PF and international sanctions compliance, the sole participant of the Company performs the following main functions:

- Approves the Company's internal legal acts related to AML/CFT and international sanctions compliance, including the annual work plan of the Internal Monitoring Unit;
- Oversees the implementation of necessary measures for risk identification, assessment, and review in the AML/CFT and sanctions compliance sector, as periodically reviewed by the IMU;
- Monitors the implementation and effectiveness of an internal control system developed and maintained by the executive body for AML/CFT and sanctions compliance;
- Reviews and approves measures aimed at addressing deficiencies identified through audits or other inspections in the AML/CFT and sanctions compliance field, issues instructions for remediation, and monitors their execution;
- Receives, discusses, and approves reports submitted by the IMU at least semiannually;

[1] *The responsible employees are the Company's frontline employees: employees of the Company's service providing departments, customer relations, business block, and post-operational departments.*

- Provides consent for the appointment and dismissal of the Internal Monitoring Body by the executive body;
- Performs other functions as prescribed by the Law, this Policy, and legal acts adopted based on the Law.

2.4. The Executive body of the Company performs the following main functions in the AML/CFT and international sanctions compliance domain:

- Ensures the implementation of the strategy and policy for AML/CFT and sanctions compliance as approved by the Company’s Sole Participant;
- Implements and manages internal processes for risk identification, assessment, monitoring, and control related to AML/CFT and sanctions compliance;
- Ensures full and effective application of the Law and other legal acts adopted based on this Policy and supervises compliance with them;
- Ensures proper training of Company employees in AML/CFT and sanctions compliance;
- Is responsible for the implementation and ongoing effective performance of the AML/CFT and sanctions compliance policy and processes approved by Sole Participant;
- Implements measures to address deficiencies identified by the IMU, including those revealed through audits or other inspections;
- Ensures the IMU is provided with the necessary human and technical resources;
- Carries out other functions as defined by the Law, this Policy, and other legal acts regulating the AML/CFT domain.

DUTIES AND AUTHORITY OF INTERNAL MONITORING BODY

2.5. The duties of the Internal Monitoring Body within the Company are aimed at preventing money laundering and terrorism financing (ML/TF), as well as establishing effective processes to respond to international sanctions, including:

2.5. 1 Implementation of mechanisms for customer identification, due diligence, and data updates, conducting ongoing and transaction monitoring, and inspections;

2.5. 2 Implementation and application of AML/CFT risk-based approach;

2.5. 3 Submission of information and reports as required by the legislation of the Republic of Armenia;

2.5. 4 Organization of the retention of documents and information necessary for the organization of AML/CFT efforts;

2.5. 5 Organization of staff training aimed at enhancing the effectiveness of AML/CFT and international sanctions compliance;

2.5. 6 Implementation and oversight of the Company’s compliance process with international sanctions.

2.6. The implementation of the AML/CFT system within the Company (including the development, revision, and submission of internal legal acts for approval by the sole participant and the executive body) and its supervision are carried out by the IMU. In its activities, the IMU is guided by the legislation of the Republic of Armenia, international standards and requirements, the Company’s Charter, this Policy, the Company’s internal legal acts, instructions of the sole participant, and the orders and directives of the executive body.

2.7. The head and employees of the IMU, when performing their functions defined by this Policy and internal legal acts adopted on its basis, are independent and hold senior management status.

2.8. The head and employees of the IMU have the right to directly report to the sole participant of the Company any issues arising in the area of AML/CFT and international sanctions compliance. They are also entitled to participate in discussions held by the sole participant and the executive body related to AML/CFT matters.

2.9. The head and employees of the IMU have direct and immediate access to all information and documentation obtained and maintained by the Company as required under the legislation of the Republic of Armenia and this Policy, including all documents related to customer accounts and conducted transactions.

2.10. The head and employees of the IMU 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.

2.11. **The Internal Monitoring Unit**

2. 11. 1 Conducts risk assessments of customers, transactions, and business relationships;

2. 11. 2 Carries out analyses for the purpose of identifying suspicious transactions or business relationships and retains the results of such analyses;

2. 11. 3 Classifies transactions or business relationships as suspicious, suspends, rejects, or terminates their execution, and freezes property of persons related to terrorism or the

proliferation of weapons of mass destruction—acting as the final decision-making authority;

2. 11. 4 Ensures the submission, on behalf of the Company, of reports on reportable transactions and suspicious transactions or business relationships to the Central Bank of Armenia (CBA);

2. 11. 5 Provides advice and assistance to the sole participant and the executive body in performing their functions related to AML/CFT and international sanctions compliance;

2. 11. 6 Conducts training for the Company's employees in the areas of AML/CFT and international sanctions (covering AML/CFT legislation, the Company's internal legal acts related to sanction requirements, and practical examples);

2. 11. 7 Performs AML/CFT risk assessments in cases of launch of new products or services, new delivery channels for existing products, or financial instruments and processes, including in cases of material changes. The risks set out in this clause must be identified and assessed before offering new types of services or implementing new service delivery channels or applying new or developing technologies;

2. 11. 8 Regularly, but no less than once every six months, reviews the compliance of conducted transactions, established business relationships, and employee actions with the Law, this Policy, and the Company's internal legal acts adopted on the basis thereof. The IMU submits reports to the executive body and the sole participant on the results of these reviews, as well as on any other matters raised by the CBA;

2. 11. 9 The IMU makes final decisions on classifying a transaction or business relationship as suspicious, suspending, rejecting, or terminating it, or freezing the property of persons related to terrorism. It also ensures the submission of reports required by law and this Policy to the CBA and performs other functions defined by the Company's internal legal acts;

2.11.10 The IMU informs the executive body and the sole participant about its decision to classify a transaction or business relationship as suspicious, suspend it, or freeze property related to terrorism, after submitting the relevant report to the CBA;

2. 11. 11 AML/CFT prevention is the responsibility of every employee of the Company. All employees are required to immediately inform the IMU if, in the course of their activities,

they become aware of any suspicious transactions involving a customer, agent, authorized person, or any third party involved in a business relationship;

2. 11. 12 All instructions, directives, and orders issued by the head of the IMU related to AML/CFT must be followed by all employees of the Company. Information related to such instructions shall be retained for at least five (5) years, unless a longer period is established by the Company's internal legal acts.

CHAPTER 3. RISK-BASED APPROACH AND RISK MANAGEMENT

3.1. For the purpose of a comprehensive presentation of the AML/CFT risk management system within the Company, this Policy outlines the main principles for mitigating ML/TF risks and ensuring compliance with sanctions. Detailed processes, tools, and related matters regarding ML/TF risk management are described in the Company's other internal legal acts (AML/CFT Compliance Procedure).

3.2. The assessment of potential and existing AML/CFT risks is carried out based on the Company's inherent AML/CFT risk and the evaluation of its internal control system aimed at managing those risks. As a result, the Company assesses the residual AML/CFT risk inherent to its operations in order to distinguish between acceptable and unacceptable risks and implement an appropriate risk management framework. Potential and existing AML/CFT risks are reviewed at least once a year.

3.3. The Company determines the AML/CFT risk level for each customer. Company employees are responsible for carrying out risk monitoring, detection, assessment, analysis, and implementation of risk mitigation/prevention measures.

3.4. The AML/CFT risk assessment of a customer by Company employees is based on the analysis of available information/documents regarding the customer, the customer's activities, and the transactions executed by the customer.

3.5. For effective risk management during customer due diligence process, AML/CFT risk is categorized as high, medium, or low, based at a minimum on the following components:

- Country or geographical risk,
- Customer, transaction, or business relationship risk,
- Product, service, or delivery channel risk.

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

3.7. Simplified due diligence may not be applied in cases where a transaction or business relationship is deemed suspicious, or when a high-risk AML/CFT criterion is present—except when the transaction involves a low-risk activity and does not exceed 1,000 times the minimum monthly wage.

If a new risk criterion arises during the course of a business relationship with a customer, the responsible employee must inform the IMU and obtain its opinion for re-assessing the risk and implementing due diligence measures aligned with the newly determined risk level.

CHAPTER 4. MINIMUM RULES 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 defined by this Policy and other internal legal acts of the Company, and verifying the customer's identity, including through remote identification. Based on the information obtained for identification purposes, the Company may verify the customer's identity during or after establishing the business relationship, within a reasonable period not exceeding seven days, provided the risk is effectively managed and such delay is necessary to avoid disrupting the normal course of the business relationship.

4.2. The Company does not establish or continue a business relationship with foreign individuals who, having no economic and/or personal interest in Armenia, fail to provide reasonable information substantiating the economic or other lawful rationale for channeling financial flows through the Armenian financial system.

4.3. Customer due diligence begins from the moment the customer applies to the Company to establish a business relationship and continues until the termination of the contractual relationship between the customer and the Company.

4.4. Customer due diligence includes the collection, analysis, and evaluation of information about the customer based on the data the Company already holds.

4.5. The Company may establish a business relationship with a customer only after obtaining the required information (including documents) for identification and verifying the customer’s identity.

4.6. The Company must determine whether the customer is acting on their own behalf or on behalf of another person and take steps to identify and verify the customer’s beneficial owner.

4.7. Enhanced due diligence is carried out in at least the following cases:

- when establishing a business relationship with the customer, the beneficial owner, or an authorized representative of the customer;
- when there are doubts about the authenticity or completeness of previously obtained customer identification information (including documents);
- when there are suspicions from an AML/CFT perspective.

4.8. If factors indicating a low level of risk are present, the Company may apply simplified due diligence to the customer’s transactions and business relationships.

4.9. Simplified due diligence may not be applied if the customer’s transactions or business relationships meet any criteria of suspicion.

4.10. If the customer’s risk is neither high nor low, it shall be classified as medium.

4.11. In case of medium-risk customers, the Company shall continuously perform appropriate due diligence on their transactions and business relationships.

4.12. In the presence of high-risk factors, the Company conducts enhanced due diligence on the customer’s transactions and business relationships. Enhanced due diligence is also applied when high-risk indicators are revealed or arise during the course of the transaction or business relationship:

4.13. In addition to those defined by Armenian legislation, high-risk indicators are described in related internal legal act of the Company and its Risk Appetite paper.

4.14. Information about the customer and their transactions (including information on beneficial owners) is updated with the following frequency:

- Low risk – once every 2 years;
- Medium risk – once a year;
- High risk – once every 6 months;
- Politically Exposed Person (PEP) – once every 3 months.

4.15. A Politically Exposed Person (PEP) is an individual who has held or holds a prominent public function in the state, political, or public sphere, or within an international organization (including their family members or persons closely associated with them). This category does not include persons performing middle or lower-level public functions.

4.16. For the purpose of determining whether a person is a Politically Exposed Person, the Company may collect information from public sources and private databases containing information about PEPs.

CHAPTER 5. SUSPENSION OF SUSPICIOUS TRANSACTION OR BUSINESS RELATIONSHIP, REJECTION OR TERMINATION OF TRANSACTION OR BUSINESS RELATIONSHIP, AND FREEZING OF PROPERTY OF PERSONS ASSOCIATED WITH TERRORISM OR PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

5.1. A transaction may be deemed suspicious both at the time of its execution (while providing services to the client) and during ongoing due diligence when monitoring client's transactions.

5.2. A transaction or business relationship, including an attempt to conduct a transaction or establish a business relationship, must be classified as suspicious and a report on the suspicious transaction or business relationship must be submitted to the Central Bank of Armenia (CBA) 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 connected to terrorism, terrorist acts, terrorist organizations, individual terrorists or terrorism financiers, or has been used or is intended to be used for terrorism or by terrorist organizations, individual terrorists, or terrorism financiers.

5.3. The issue of qualifying a transaction or business relationship as suspicious and submitting a report to the CBA is considered in the following cases.

5.3.1 When the situation under consideration fully or partially matches the indicators or typologies of a suspicious transaction or business relationship; or

5.3.2 When it becomes evident that, although the transaction or business relationship (concluded or proposed) does not directly meet the suspicious indicators or typologies, the rationale, dynamics, or other circumstances of the transaction provide grounds to assume it may be conducted for ML/TF purposes.

5.4. If, as a result of the review, the transaction or business relationship is not classified as suspicious and a report is not submitted to the CBA, the rationale, conclusions, analysis process, and outcomes for not classifying it as suspicious must be documented and retained by the Company for at least five years, unless a longer period is defined by internal legal acts.

5.5. The IMU has the right to suspend the transaction or business relationship for a maximum of 5 days and is obliged to do so for 5 days upon receiving an instruction from the CBA, while simultaneously submitting the suspicious transaction or business relationship report to the CBA.

5.6. The decision of the CBA to suspend a transaction or business relationship must be executed immediately upon receipt by the Company.

5.7. A decision by the Company or the CBA to suspend a transaction or business relationship may be revoked before the expiry of the suspension period only by the CBA, either on its own initiative or based on the Company’s request, if there is no longer a need for the continued suspension.

5.8. If the Company does not receive a decision from the CBA regarding the extension of the suspension, the suspension is considered terminated.

5.9. Until information is received about the suspension being lifted, the Responsible Employee shall not execute the relevant transaction.

5.10. The transaction shall be rejected or the establishment of a business relationship shall be denied in the following cases;

5.10.1 upon receipt of relevant instructions defined by a decision of the CBA;

5.10.2 if proper customer due diligence (CDD) cannot be performed;

5.10.3 If the person is subject to international sanctions. In such cases, the client's transactions must be carried out in accordance with sanction requirements, and in the presence of risks of breaching such requirements, the transactions shall be rejected.

5.11. The transaction shall be terminated or the business relationship ended in the following case;

5.11.1 If ongoing due diligence of the customer is impossible or has failed.

5.12. In case of rejection or termination of a transaction or business relationship, the issue of classifying them as suspicious must also be considered.

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

5.14. Property directly or indirectly owned or controlled by persons associated with terrorism or the proliferation of weapons of mass destruction, as listed by UN Security Council resolutions or the CBA, shall be frozen immediately without prior notice to the persons involved. The CBA publishes the list of such persons on its website.

5.15. If the Company has information indicating that a person corresponds to the definition of a person associated with terrorism or the proliferation of weapons of mass destruction, it is obliged to inform the CBA immediately.

5.16. If the property of persons associated with terrorism or the proliferation of weapons of mass destruction is frozen, the transaction or business relationship shall immediately be classified as suspicious and a report submitted to the CBA.

5.17. All employees of the Company, regardless of their position, are prohibited from disclosing or making known to any person the fact of submitting a report or any other information to the CBA regarding a client and/or transaction, including the classification, suspension, or freezing of a transaction or business relationship, as well as the fact that a client is included in the "Black List."

CHAPTER 6. RECRUITMENT OF INTERNAL MONITORING BODY AND TRAINING OF THE STAFF

6.1. Training on AML/CFT and compliance with international sanctions for the Company's employees, including the sole participant, the executive body, and internal audit, shall be organized at least once a year. For newly hired employees, training shall be provided within three months from the date of hire. To assess the effectiveness of the training, questions related to AML/CFT and international sanctions compliance are included in the qualification tests (certification exams) for both new and existing employees.

6.2. The IMU develops and annually updates the Company's employee training program, which must mandatorily include changes in Armenian legislation on AML/CFT, regulations related to compliance with international sanctions, information on the implementation and updates of such regulations within the Company, and a training schedule. This schedule is presented for approval by the sole participant within the framework of the IMU’s annual program.

6.3. The IMU may also organize separate thematic, specialized training courses, tests, and discussions.Training materials, information about participating employees, and documents confirming their participation must be recorded and kept for at least five (5) years, unless a longer retention period is set by the Company’s internal legal acts.

6.4. Head of IMU may be a person who:

- Has a higher education and an internationally recognized professional qualification in the financial sector,
- Has at least one (1) year of work experience in AML/CFT or at least five (5) years of managerial experience related to banking/investment operations,
- Is knowledgeable in the AML/CFT legislation of the Republic of Armenia and related normative legal acts, international standards in the AML/CFT field, and internal control rules,
- Has knowledge of FATF recommendations as well as principles set by international organizations in the field of AML/CFT risk assessment; international qualification is considered an advantage,
- Communicates fluently in Armenian and Russian, and has proficiency in English.

CHAPTER 7. PRINCIPLES AND PROCEDURES FOR COMPLIANCE WITH INTERNATIONAL SANCTIONS

7.1. International sanctions (hereinafter referred to as "Sanctions") are established through international legal acts adopted by international and intergovernmental organizations, international treaties between countries, laws and other legal acts adopted by state authorities of various countries. The IMU regularly monitors these sources.

7.2. When providing services to clients, relevant departments of the Company take measures to ensure compliance with sanctions imposed by the UN, US, EU, and United Kingdom, and, if necessary, other countries, their respective authorities, international and intergovernmental organizations.

7.3. The Company adheres to the following sanctions:

7.3.1 Restrictions applied to specific countries;

7.3.2 Restrictions related to goods and/or sectors of activity in certain countries or territories;

7.3.3 Restrictions imposed on individuals;

7.3.4 Asset freezing requirements.

7.4. The Company's management ensures the implementation of necessary measures to comply with the international restrictions and sanctions requirements established by the Policy.

7.5. Company employees are required to provide services to customers in accordance with the Company's approach toward country-based restrictions, sectoral restrictions, and restrictions on goods/services related to specific countries or territories.

7.6. The Executive Body ensures the enforcement and monitoring of international restrictions and sanctions requirements within the Company, including employee training and awareness-raising.

7.7. The Company ensures compliance with international sanctions requirements in relationships with customers, partners, service providers, including partner financial institutions, depositary service providers, suppliers, and all types of third parties.

7.8. In case of ambiguity in interpreting sanction-related requirements, the implementation of sanction provisions is subject to interpretation by the IMU, with legal and compliance units involved as necessary:

7.9. Based on the approach of partner financial institutions, potential risks arising from international sanctions, and business best practices, the IMU may recommend applying a stricter approach than required, if deemed necessary to reduce reputational and financial risks.

7.10. Coordination of compliance with international sanctions, implementation thereof, staff training, tools and processes related to challenges in this area is carried out by the IMU.

7.11. Regardless of their position, all Company employees are prohibited from assisting, facilitating, remaining passive, altering, concealing information, or providing advisory services to clients for the purpose of evading sanctions requirements.

7.12. The Company uses a dedicated database to screen for matches against individuals listed under international sanctions or designated by competent authorities.

7.13. Any inconsistencies related to compliance with international sanctions, inquiries or requests from third parties must be immediately reported t thoe IMU.

7.14. The IMU assists in preparing responses to inquiries received from sanction supervisory authorities and partner financial institutions regarding international sanctions compliance matters.

7.15. If an individual or legal entity holds 50% or more participation in a legal entity and is directly or indirectly subject to sanctions, the legal entity is also considered as a subject of international sanctions. In such cases, the IMU may apply a stricter approach, including enhanced customer due diligence, taking into account legal requirements, business practices, risks arising from the transaction (or business relationship), approaches of international partners, and cases where full information about all beneficial owners is unavailable or there are doubts about the true beneficial owner.

7.16. When establishing business relationships or concluding transactions with persons listed under international sanctions, the Company follows the applicable sanction requirements and provisions of the relevant legal act, along with any related interpretations or clarifications.

7.17. In transactions involving persons subject to international sanctions or listed in relevant databases, or where connected parties are involved, the final decision is made following a discussion initiated by the IMU with the Executive Body and, if needed, other designated stakeholders. The discussion and final decision must be documented.

7.18. The Company’s transaction screening under international restrictions and sanctions includes at minimum the collection and analysis of the following information:

7.18.1 Determination of the client’s residency and assessment from a sanction’s perspective;

7.18.2 Identification of the center of vital interests for foreign clients, assessed from a sanctions perspective;

7.18.3 Other third parties, partners, involved countries, currency, source and purpose of funds, nature of goods/services, business activity and economic rationale, and other factors including citizenship, place of birth, residence, etc., that the IMU or the financial institution executing the transaction deems significant in evaluating potential sanctions evasion.

7.19. Prior to establishing partnership relations, the Company, as part of the due diligence process, identifies the potential partner's approach and policy regarding sanctions compliance and risk-based implementation of relevant legal acts.

7.20. If, at any time, a client or any of their transactions becomes subject to international sanctions, the Company must apply the required sanction measures within a reasonable timeframe, including terminating the business relationship and/or rejecting transactions, if necessary, in accordance with applicable legislation. This applies equally to partner financial institutions, suppliers, and other cooperating parties.

7.21. For transactions (or business relationships) that present a high risk of violating sanctions requirements, the Company may decide to reject the transaction or establishment of a business relationship, or to terminate an existing one. The final decision is made through a discussion initiated by the IMU with the Executive Body and, if necessary, other designated stakeholders. The results of the discussion and final decision must be documented.

CHAPTER 8. OTHER PROVISIONS

8.1. Failure by the Company to comply with the requirements of the Law or legal acts adopted based on the Law, or improper compliance therewith, shall lead to liability measures as defined by the legislation regulating their activities, in accordance with the legislation of the Republic of Armenia.

8.2. This Policy is subject to revision in the event of changes in the legislation of the Republic of Armenia, standards and requirements in the field of AML/CFT, as well as in other necessary cases.

8.3. The Company or its employees (including managers) shall not be subject to property liability for proper performance of their duties as prescribed by the Law, nor shall they bear criminal, administrative, or other liability for proper performance of their duties under the Law.

8.4. All employees of the Company must get familiarized with this Policy.

8.5. This Policy shall be submitted to the Central Bank of Armenia via the CBANet system within one week following its approval.