A P P R O V E D

by the decision No. 2024/1 of the General Meeting of

CUBE INVEST CJSC dated January 23, 2024.

Meeting Chairman:

Armen Ter-Hakobyan----------

Cube Invest CJSC
Anti-Money Laundering and
Combating the Financing of Terrorism

POLICY

2024

CHAPTER 1. GENERAL PROVISIONS

1.1 The Anti-Money Laundering and Combating the Financing of Terrorism Policy (hereinafter referred to as the "Policy") has been developed in accordance with the Law of the Republic of Armenia "On Combating Money Laundering and Financing of Terrorism" (hereinafter referred to as the "Law"), the normative legal acts adopted by the Central Bank of the Republic of Armenia (hereinafter referred to as the "Authorized Body") and the amendments and additions made thereto respectively, FATF standards, international best practices and the requirements of the internal legal acts of CUBE INVEST CJSC (hereinafter referred to as the "Company").

1.2 The Policy defines the policy pursued by the Company to counter money laundering and financing of terrorism, as well as international sanctions, the mandatory measures and procedures implemented that will exclude the circulation of criminally obtained income and the financing of terrorism through the Company, and the circumvention of international sanctions.

1.3 The Policy defines the measures aimed at their prevention, the procedure for collecting, recording, and storing information on suspicious transactions, and the duties and responsibilities of the Company's employees related to the implementation of this Policy.

1.4 The Company pursues a policy that maximally excludes the investment or circulation of funds obtained through criminal means and serving as a source of financing terrorism in the Company.

1.5 The Policy applies throughout the entire system of the Company, and provisions thereof extend to all management bodies, structural subdivisions, their managers, and employees of the Company. All employees of the Company, regardless of their position, shall adhere to the principles established by the Policy and demonstrate their honesty, accountability, and business ethics in all relationships with customers, competitors, partners, shareholders of the Company, state and supervisory bodies, and among themselves.

CHAPTER 2. MAIN CONCEPTS AND ABBREVIATIONS USED IN THE POLICY

The main concepts used in this Policy, as well as in other internal legal acts adopted based thereon, are:

Law	The Law of the Republic of Armenia "On Combating Money Laundering and Financing of Terrorism."
Property	According to the Criminal Code of the Republic of Armenia, any type of material goods, movable or immovable objects of civil law, including financial (monetary) funds, securities and property rights, documents, or other means certifying property rights or interests, interest, dividends, or other income received from the property or accrued thereon, as

	well as related and patent rights.
Money Laundering (ML)	The conversion or transfer of property obtained through criminal means (if it is known that such property was obtained as a result of criminal activity), which was intended to conceal or distort the criminal origin of that property or to assist any person in avoiding responsibility for the crime committed by him/her, or to conceal or distort the true nature, source, location, method of disposal, movement, rights or ownership of the property (if it is known that such property was obtained as a result of criminal activity) or to acquire, possess, use or dispose of the property (if at the time of receiving that property it was known that it was obtained as a result of criminal activity).
Financing of Terrorism (FT)	The direct or indirect provision or collection of property, by any means, with the knowledge that it shall be used or may be used, in whole or in part, for terrorism or hostage-taking/keeping, or by a terrorist organization or an individual terrorist, or the provision of financial services with the knowledge that those services are aimed at committing terrorism or hostage-taking/keeping, or that results thereof will be used by a terrorist organization or an individual terrorist.
Financing of Proliferation of Weapons of Mass Destruction (FPWMD)	The provision or collection of property or the provision of financial services for the proliferation of weapons of mass destruction (creating, producing, acquiring, developing, possessing, transporting, or selling chemical, biological, nuclear, or other types of weapons of mass destruction prohibited by international treaties, as well as special means of their transportation, using special means of transportation of weapons of mass destruction prohibited by international treaties, transferring raw materials or special fissile materials to a state that does not possess nuclear weapons, providing weapons of mass destruction prohibited by international treaties or components necessary for their production) or for the purpose of using or testing weapons of mass destruction prohibited by international treaties of the Republic of Armenia.
Person related to terrorism	Any individual terrorist, including a person suspected, accused, or convicted of terrorism or attempted terrorism, or

	a terrorist organization, a person affiliated therewith, a person acting on their behalf or under their instructions, or directly or indirectly owned or controlled thereby, who has been included in the lists published by the UN Security Council resolutions or in accordance therewith or by the Central Bank of the Republic of Armenia. For the purposes of the Policy, this definition also includes persons related to the proliferation of weapons of mass destruction.
Senior Management	The unit responsible for the Company's fight against ML/TF (Money Laundering/Terrorist Financing), which is authorized to make decisions and take actions on behalf of the Company on ML/TF prevention issues.
Transaction	A transaction between the Company and the customer or authorized person, as well as between the customer or authorized person and another person, which is carried out through the Company or is the subject of study/observation by the reporting entity. Any action that creates, modifies, or terminates rights and obligations based on or as a result of a certain transaction can also be considered a transaction.
Business Relationship	Periodic services provided by the Company to the customer, which are not limited to one or several one-time transactions.
Vital Interests Center	A place where an individual's family or economic interests are concentrated. Family or economic interest may be manifested in the place where the person's residential house (apartment) is located, where the person and/or his/her family resides, where his/her (family's) personal or family main property or the place of main economic (professional) activity is situated.
Customer	A person who establishes or maintains a business relationship with the Company, as well as a person who offers the Company to perform or who performs a one-time transaction.
Authorized Person	A person who has the authority to perform transactions or carry out certain legal or factual actions in a business relationship on behalf of and by the instruction of the Customer, including a person who acts as a representative based on the powers granted by the Customer through a power of attorney or other grounds established by law.
Legal Entity	An organization/institution that has the status of a legal entity under the legislation of the Republic of Armenia and/or

	foreign legislation, as well as a legal formation that does not have the status of a legal entity under foreign legislation.
Beneficial Owner	A natural person on whose behalf or for whose benefit the customer actually acts, and/or who actually controls the customer or the person on whose behalf or for whose benefit the transaction is being carried out or the business relationship is being established. In the case of a legal entity (except for a trust or other legal formation that does not have the status of a legal entity under foreign legislation), the beneficial owner is also considered to be a natural person who: - directly or indirectly owns 20 (twenty) percent or more of the voting shares (stocks, shares) of the given legal entity, or directly or indirectly has a 20 percent or more participation in the authorized capital of the legal entity, - exercises actual control over the given legal entity by other means, or - is an official who carries out the general or current management of the given legal entity's activities in cases where there is no natural person who meets the requirements of the above-mentioned points of this definition.
Customer Business Profile	The totality of the Company's information (perceptions) about the nature, influence, and significance of the Customer's activities, the existing and expected movement, volumes, and areas of business relationships and one-time transactions, the presence of authorized persons and beneficial owners, the nature of their identity and interconnectedness, as well as other facts and circumstances related to the Customer's activities.
Politically Exposed Person (PEP)	A person who has performed or performs significant functions of a state, political, or public nature, as well as in an international organization (including a family member or a person closely associated therewith).
Suspicious Transaction or Business Relationship	A transaction or business relationship, including an attempt to conduct a transaction or establish a business relationship, in which it is suspected or there are sufficient grounds to suspect that the property has been obtained through criminal

	means or is related to terrorism, terrorist acts, terrorist organizations, individual terrorists, or those who finance 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 those who finance terrorism.
Shell Bank	A bank that, despite being founded, registered, licensed, or otherwise incorporated in a country, is not actually managed or does not have a physical presence or place of operation in that country, and is not affiliated with any group of financial institutions that are subject to effective consolidated supervision and engage in regulated activities.
Customer Due Diligence (CDD)	The process of obtaining and analyzing information (including documents) about the customer's identity and business profile by the Company, applying a risk-based approach, in order to form a proper understanding of the customer. It includes: 1. Identification and verification of the identity of the Customer (including the authorized person and beneficial owner), 2. Clarification of the purpose and intended nature of the transaction or business relationship, and 3. Ongoing due diligence of the business relationship.
Counterparty	The other participant in a transaction carried out by the Customer, who provides (transfers) or to whom the property resulting from the transaction is addressed.
Risk	A circumstance indicating the likelihood of ML/TF, which can be characterized according to countries or geographic locations, types of customers, types of transactions or business relationships, types of services, or other criteria.
High-Risk Criterion	A high-risk criterion is a criterion defined by the legislation of the Republic of Armenia, as well as by the internal legal acts of the Company, which indicates a high probability of ML/TF.
Non-Face-to-Face Transaction, Business Relationship	A business relationship established with a customer where the entire process of establishing the business relationship and conducting the transaction, including making the corresponding payments, takes place without face-to-face contact, including on online platforms.
Enhanced Customer Due Diligence	An extended application of the customer due diligence process by the Company, in which case, in addition to the actions

	defined by customer due diligence, it is also necessary to at least: 1. Obtain senior management approval before establishing a business relationship with the customer, continuing the business relationship, as well as in cases where it is subsequently revealed that the customer or the beneficial owner is characterized by a high-risk criterion, or the transaction or business relationship includes such a criterion, 2. Take necessary measures to clarify the source of income and assets of the customer, as well as the beneficial owner who is a PEP, 3. Examine the preconditions and purpose of the transaction or business relationship in as much detail as possible, and 4. Carry out ongoing enhanced monitoring in the case of a PEP.
Low-Risk Criterion	A criterion defined by the legislation of the Republic of Armenia that indicates a low probability of ML/TF. Exceptions are units located in Non-Compliant, Offshore, Sanctioned, or Corruption-Risk Countries or Territories.
Simplified Customer Due Diligence	A limited application of the customer due diligence process by the Company, in which case the following information is collected when performing identification and identity verification: 1. For an individual - name, surname, identity document details, 2. For a legal entity - name and identification number (state registration, registration number, etc.), and 3. For an individual entrepreneur - name, surname, identity document details, identification number (state registration, registration number, etc.), and for a state body and local self-government body - full official name.
Medium-Risk Criterion	The risk is assessed as medium (standard) in the absence of high or low-risk criteria.
International Sanctions	International restrictions, prohibitions, embargoes, and asset freezing requirements of a commercial, economic, and financial nature applied to countries or territories, types of goods and/or spheres of activity, and persons against certain individuals, countries, and/or organizations, aimed at preventing activities and behavior by the latter that pose a

	universal threat to international security.
Blacklist	Lists adopted and published by the Central Bank of the Republic of Armenia, UN Security Council, OFAC, European Union, and other bodies regarding persons involved in the organization and implementation of ML/TF and the proliferation of WMD.
Suspension of a Transaction, Business Relationship	A temporary prohibition on the actual and legal movement of property subject to a suspicious transaction and/or business relationship.
Refusal to Conduct a Transaction or Establish a Business Relationship	Non-performance of actions intended for conducting a transaction or establishing a business relationship.
Seizure of property	The direct or indirect freezing of assets belonging to or controlled by persons linked to terrorism, and/or the imposition of a moratorium on the movement of such assets, including their direct or indirect ownership, use, or disposal, as well as the prohibition of the establishment or continuation of any commercial relationship (including the provision of financial services) or the conclusion or performance of transactions with such persons.
FATF (Financial Action Task Force)	An intergovernmental independent body that develops policies to protect the global financial system from ML/TF (Money Laundering/Terrorist Financing) and FPWMD (Financing of Proliferation of Weapons of Mass Destruction), and supports their implementation.
Non-compliant country or territory	A foreign country or territory that does not apply or improperly applies the international requirements for combating ML/TF (Money Laundering/Terrorist Financing), in accordance with the lists published by the Central Bank of the Republic of Armenia (RA CB) and the FATF (Financial Action Task Force).
Offshore country or territory	An offshore country or territory published by the Central Bank of the Republic of Armenia (RA CB), a country or territory with special liberal taxation systems published by the Government of the Republic of Armenia and (or) international organizations.
Country with high corruption risk	A country where a high level of corruption has been assessed according to the "Corruption Perceptions Index" ranking by

	"Transparency International" organization and (or) according to the ranking published by another international organization.
Typology	A possible scheme describing the logic and sequence of actions and (or) steps aimed at ML/TF (Money Laundering/Terrorist Financing) and FPWMD (Financing of Proliferation of Weapons of Mass Destruction), as defined by the legal acts of the Central Bank of the Republic of Armenia (RA CB), as well as by the internal legal acts of the Company.
ML/TF residual risk	The final component of the strategic analysis of ML/TF (Money Laundering/Terrorist Financing) risks inherent to the Company's activities, which is formed as a result of the assessment of ML/TF inherent risk and the effectiveness of the internal control system.
Company's management body	Executive Director, Board of Directors (if available), General Meeting of Shareholders.
Internal monitoring body	A subdivision or employee of the Company engaged in ML/TF (Money Laundering/Terrorist Financing) prevention and compliance with sanctions, or a specialized person carrying out the relevant activities.
Customer Service Department Employee (CSDE)	An employee of the Company who participates in the process of customer identification and due diligence, including performing online customer identification, opening accounts, concluding contracts, and ongoing customer service.
RA CB	Central Bank of the Republic of Armenia
FMC	Financial Monitoring Centre
IOB	Internal Observations Body

CHAPTER 3. PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM IN THE COMPANY

3.1 The company's management is responsible, in the manner prescribed by the legislation of the Republic of Armenia, for the proper implementation of the internal legal acts adopted in the Company for combating money laundering and terrorist financing, the awareness of employees regarding the procedures and requirements established therein, as well as for giving employees instructions that lead to violations of the legislation of the Republic of Armenia and the internal procedures of the Company.

3.2 The company's management ensures that the employees carrying out the functions defined by the Policy acquire qualifications based on the professional competence criteria established by

the Central Bank of the Republic of Armenia and/or internal legal acts, and meet other criteria established by the Company and the Authorized Body. The criteria established by the Company are:

3.2.1 The employee of the Internal Observations Body shall have a higher education and at least 1 year of work experience in the financial system, and the head of the Internal Observations Body shall have at least 3 years of professional work experience.

3.2.2 The head of the Internal Observations Body and the senior specialist (if any) shall have an international professional qualification provided by well-known associations in the field (ICA, ACAMS), and the Internal Observations Body specialist shall have a professional qualification of the Internal Observations Body provided by the Union of Banks of the Republic of Armenia.

3.2.3 The following persons cannot be employees of the Internal Observations Body:

1) Those who have committed an intentional crime, the conviction for which has not been removed or expunged in the prescribed manner,

2) Those who have been deprived by a court decision of the right to hold positions in the financial, tax, customs, commercial, economic, and legal fields,

3) Those who have been declared bankrupt and have outstanding (unforgiven) liabilities,

4) Those who are involved in a criminal case as a suspect, accused, or defendant,

5) Those who have a negative business reputation in the financial system,

6) Those who do not meet the requirements established by paragraph 3.2 of this Policy, and

7) Those who are related to the managers of the Company.

3.3 The implementation (including the development, review, and submission for approval of internal legal acts) and supervision of the ML/TF system in the Company is carried out by the Internal Observations Body, which in the course of its activities is guided by the legislation of the Republic of Armenia, international standards and requirements, the Articles of Association of the Company, this Policy, the internal legal acts of the Company, the orders and instructions of the Executive Director.

3.4 General Meeting of the Company:

3.4.1 establishes the Policy, approves the internal legal acts on ML/TF prevention, as well as the charters and/or regulations of the divisions carrying out these functions,

3.4.2 agrees to the appointment or dismissal of ML/TF responsible employees by the Chief Executive Officer,

3.4.3 approves the Company's annual program for ML/TF prevention, discusses and approves reports on the implementation of this program, and establishes control over the implementation of these programs,

3.4.4 approves the annual programs of the Company's internal audit in the areas of ML/TF prevention, as well as reports on their implementation,

3.4.5 discusses and approves the conclusions revealed as a result of the Company's internal and external audits and/or other inspections in the field of ML/TF prevention, as well as the programs of measures aimed at eliminating the identified shortcomings, and monitors their implementation,

3.4.6 if necessary, instructs the Internal Observations Body responsible person to conduct

studies/inspections within the Company on the functions defined by the Policy, discusses and approves the measures aimed at eliminating the identified shortcomings and oversees their implementation,

3.4.7 with the established frequency, but no later than once every six months, discusses and approves the reports of the Internal Observations Body related to the Company's ML/TF prevention activities.

3.5 The Executive Director of the Company:

3.5.1 carries out the process of hiring and/or dismissing Internal Observations Body employees,

3.5.2 ensures the full and effective implementation, application, and oversight of the requirements of the legislation on ML/TF prevention in the Republic of Armenia and the internal legal acts of the Company, including this Policy.

3.5.3 ensures proper training of the Company's employees in the field of ML/TF prevention.

3.5.4 ensures the availability of adequate and sufficient material, technical, software, and other resources for the effective implementation of the ML/TF prevention system.

3.5.5 ensures the implementation of measures aimed at eliminating the shortcomings identified as a result of studies and inspections in the field of ML/TF prevention.

3.6 The Company's ML/TF risk management system is based on a three-line model of control, where the functions of the first line of control in the fight against ML/TF are assigned to the CDD and Responsible Employees, and the functions of the second line of control are assigned to the Internal Observations Body.

3.7 Employees of the Internal Observations Body, in carrying out the functions defined by the Policy and the internal legal acts adopted based thereon, shall be independent and have the status of Senior Management.

3.8 Employees of the Internal Observations Body have the right to directly present to the governing bodies of the Company the problems that have arisen in the field of the Company's fight against ML/TF, as well as to participate in the discussion of issues related to combating ML/TF by the governing bodies of the Company.

3.9 Employees of the Internal Observations Body shall have direct and immediate access to the information acquired and maintained by the Company in accordance with the legislation of the Republic of Armenia and the Policy, including all documents related to customer accounts and transactions.

3.10 Employees of the Internal Observations Body have the right to request clarifications from any employee of the Company regarding transactions or business relationships, as well as information about customers, authorized persons, and beneficial owners.

3.11 Internal Observations Body:

3.11.1 ensures the assessment of the customer's and the transaction's or business relationship's risk.

3.11.2 conducts analyses for the purpose of identifying suspicious transactions or business relationships, and maintains the results.

3.11.3 carries out the qualification as suspicious, suspension, refusal of execution or termination

of transactions or business relationships, and the freezing of the assets of persons related to terrorism and the proliferation of weapons of mass destruction, being the final decision-maker.

3.11.4 ensures the submission of reports on mandatory notification transactions, suspicious transactions, or business relationships on behalf of the Company to the Central Bank of Armenia.

3.11.5 provides advice and assistance to the management bodies and employees of the Company in carrying out their functions related to ML/TF prevention.

3.11.6 conducts training of the Company's employees in the field of AML/CFT (AML/CFT legislation, relevant internal legal acts of the Company, practical examples).

3.11.7 assesses the ML/TF risks in the case of the introduction of new products, financial instruments, processes, and/or their significant changes in the Company.

3.11.1 ensures the assessment of the customer's and the transaction's or business relationship's risk.

3.11.8 periodically, but no later than once every six months, studies the compliance of the Company's performed transactions and approved business relationships, the actions of the Company's employees with the Law, the Policy, and the Company's internal legal acts adopted based thereon. The Internal Observations Body presents a report on the results of the study, as well as other issues raised by the Central Bank of Armenia, to the governing bodies of the Company.

3.11.9 ensures the implementation of other operations and responsibilities defined within the framework of the subdivision's responsibilities by the legislation of the Republic of Armenia and the Company's internal legal acts.

3.12 the Internal Observations Body makes the final decision on qualifying as suspicious, suspending, rejecting the implementation or terminating the transaction or business relationship, freezing the property of persons associated with terrorism, as well as ensuring the provision of reports to the Central Bank of Armenia as defined by the Law and the Policy, and the implementation of other functions defined by the Company's other internal legal acts.

3.13 the Internal Observations Body informs the Company's governing bodies about its decision to qualify as suspicious, suspend, or freeze the property of persons associated with terrorism regarding the transaction or business relationship, after providing the report on the suspicious transaction or business relationship to the Central Bank of Armenia.

3.14 The prevention of ML/TF is the responsibility of every employee of the Company, and the Company's employees are obligated to immediately inform the Internal Observations Body about the presence of suspicious transactions of the customer or counterparty related to ML/TF during the course of their activities.

3.15 The letters, instructions, and orders sent by the Internal Observations Body regarding the prevention of ML/TF are subject to mandatory implementation by all employees of the Company.

3.16 The employees of the servicing subdivision and the heads of subdivisions:

3.16.1 are obligated to take measures defined by this Policy to detect and prevent suspicious transactions carried out by the Company's customers or third parties.

3.16.2 do not have the right to inform other persons, as well as the person about whom information is provided to the Company's Internal Observations Body, about the fact of providing the information.

3.16.3 cooperate with the Internal Observations responsible person for the proper implementation of the Policy's requirements.

3.17 The Company submits to the Authorized Body the information related to money laundering and financing of terrorism defined by the Law, other legal acts, and this Policy, including information containing a legally protected secret, in the manner prescribed by the Law, other legal acts adopted based thereon, and this Policy.

3.18 The Company provides the information specified in the Law and this Policy to the criminal prosecution authorities exclusively in the manner prescribed by the RA Law "On Bank Secrecy."

CHAPTER 4. APPLICATION OF A RISK-BASED APPROACH

4.1 For the comprehensive presentation of the ML/TF risk management system within the Company, the Policy describes the fundamental principles for mitigating ML/TF risks. The detailed processes, tools, as well as other issues arising from ML/TF risk management are described in the Company's "Procedure for Combating ML/TF and Compliance with Sanctions."

4.2 Based on the Policy, the Company's mechanisms for ML/TF risk management are formed, with the aim of timely identifying, assessing, and mitigating potential and existing ML/TF risks.

4.3 The assessment of potential and existing ML/TF risks is carried out based on the evaluation of the Company's inherent ML/TF risk and the internal control system aimed at its management, as a result of which the Company assesses the residual ML/TF risk inherent to its activities, with the aim of distinguishing between acceptable and unacceptable risks and implementing a proper risk management system. Potential and existing ML/TF risks are reviewed at least annually.

4.4 The Company identifies and assesses potential and existing risks associated with the introduction of new types of services or the implementation of new methods of service delivery, as well as the application of new or emerging technologies. Moreover, the risks defined in this clause are identified and assessed prior to the provision of new types of services or the implementation of new methods of service delivery, or the application of new or emerging technologies.

4.5 In order to manage risks effectively, the Company, in conducting a proper customer survey, assesses the risk of ML/TF as high, medium, or low.

4.6 For high-risk customers, enhanced due diligence is applied, for medium-risk customers, standard due diligence is applied, and for low-risk customers, simplified due diligence may be applied.

4.7 Simplified due diligence cannot be carried out in the case of a suspicious transaction or business relationship, or in the case of a high-risk ML/CFT criterion, except when there is a medium or high-risk criterion, but a low-risk transaction is carried out, which does not exceed a thousand-fold of the minimum wage.

4.8 If new risk criteria arise during business relations with a customer, the Anti-Money Laundering Reporting Officer shall inform the Internal Observations Body to assess the need for a review of that risk and a corresponding re-evaluation of the customer, taking into account the new risk factors.

CHAPTER 5. THE DISCLOSURE OF THE COMPULSORY SUBJECT TO REPORT SUSPICIOUS TRANSACTIONS OR BUSINESS RELATIONSHIPS TO THE AUTHORIZED BODY

5.1 An employee of the Company's Internal observations Body shall provide the Authorized Body with a report on any of the following transactions:

5.1.1 Non-cash transactions with a value equal to or exceeding 20 million drams.

5.1.2 Suspicious transactions or business relationships, regardless of the amount involved.

5.2 Regardless of the amount, the following transactions are not considered to be subject to reporting:

5.2.1 Transactions concluded between two professional participants in the secondary financial market, which are concluded on their own account and in their own name.

5.2.2 Transactions accomplished by the Company for its own needs, in order to ensure the Company's ongoing operations, with the exception of purchases of financial assets from its customer.

5.2.3 Changes in transactions concluded with the customer and previously presented in the statement, which do not result in a change in the amount or currency of the transaction.

5.3 In order to detect suspicious transactions and business relationships, the Internal Observations Body combines transactions/business relationships conducted in the Company against the indicators and typologies of suspicion published by the Authorized Body, however is not limited thereto.

5.4 The Company may submit a statement on a suspicious transaction or business relationship to the Authorized Body even in cases where the suspicion of that transaction or business relationship does not arise from the Law, the guidelines presented by the Authorized Body, the grounds and criteria for suspicious transactions defined in this Policy, but the rationale and dynamics of doing so provide a reason to assume that it is accomplished for the purpose of money laundering or terrorist financing.

5.5 The transaction or business relationship conducted by the company (or the employee executing the transaction) shall be considered suspicious, including the attempt to perform it, and a report about it shall be immediately provided to the Authorized Body in the case of identification of bases or criteria for a suspicious transaction or business relationship as defined by this Policy.

5.6 The business relationship or transaction shall be considered suspicious if there is suspicion or sufficient baselines to suspect that the financial means or other property involved in the business relationship or transaction are connected, or there is an intention to use them on behalf of terrorist organizations or individual terrorists for terrorist purposes.

CHAPTER 6.
PRINCIPLES OF CUSTOMER IDENTIFICATION AND DUE DILIGENCE

6.1 The Company may establish a business relationship or conduct a transaction with a customer only after obtaining the information for the customer's identification as defined by this Policy and other internal legal acts and verifying the customer's identity, including through remote identification methods.

6.2 In the Company, it is prohibited to open, issue, provide or service:

6.2.1 Anonymous or fictitious named accounts, accounts expressed solely by numeric, alphabetic, or other conditional symbols

6.2.2 Bearer securities

6.2.3 Establish or continue correspondent relationships with fake(shell) banks

6.2.4 Establish business relationships without face-to-face interaction through remote communication means with video recording for the purpose of verifying the customer's identity, including cases where the Authorized Body acts on behalf of the customer.,

6.2.5 Execution of the transaction and/or establishment of the business relationship without consideration of comparison against watchlists and lists of individuals subject to international sanctions

6.3 The Company identifies the customer and verifies his/her identity based on the originals of reliable and valid documents issued by the competent state authorities, as well as other information detailed in the Company's "ML/TF Procedures."

6.4 The Company ascertains whether the customer is acting on his/her own behalf or on behalf of and/or for the benefit of another person, and identifies the authorized Body.

6.5 The Company identifies the beneficial owner and takes reasonable steps to verify his/her identity.

6.6 For customers that are legal entities, the Company collects comprehensive information about the ownership and control structure of the legal entity, including the powers of its participants and management bodies, in order to identify the beneficial owner.

6.7 In carrying out the actions of identifying and verifying the identity of the customer (including the Authorized Person and Beneficial Owner) and ascertaining the purpose and intended nature of the business relationship, the Company may use the data obtained by another financial or non-financial institution or person as a result of CDD (Customer Due Diligence), provided that:

6.7.1 The Company shall bear ultimate responsibility for CDD (Customer Due Diligence).

6.7.2 The Company shall obtain the information intended for CDD (Customer Due Diligence) directly from another financial institution, non-financial institution, or person.

6.8 The Company shall take sufficient measures to ensure that the other financial institution, non-financial institution, or person is authorized and able to immediately provide, upon request, the information obtained as a result of the customer's due diligence, including copies of the documents.

6.9 The Company conducts ongoing due diligence on the customer's business relationship. Ongoing due diligence on the business relationship includes the Company's monitoring of transactions with customers to verify the accuracy of information about the customer, his/her business profile and risk level, the consistency of the customer's activity with such information, and, if necessary, also the legitimacy of the source of the customer's income and assets.

6.10 The Company updates the information collected within the framework of the customer's due diligence (including enhanced or simplified) at the frequency established by its internal regulations, in order to ensure the relevance and currency of such information.

6.11 In the course of business relationships with foreign financial institutions, in addition to the CDD (Customer Due Diligence) requirements, the Company:
6.9.1 collects sufficient information to fully understand the nature of the partner institution's activities and, based on public and other reliable information, assesses the business reputation of the financial institution and the quality of oversight exercised over it, including whether that financial institution has been or is currently involved in any criminal proceedings related to ML/TF (Money Laundering/Terrorist Financing).
6.9.2 assesses the ML/TF and FPWMD compliance procedures implemented by the financial institution, to ensure that they are sufficient and effective.
6.9.3. establishes the business relationship after obtaining approval from senior management.
6.9.4. understands and documents the respective ML/TF and FPWMD compliance obligations of each partner institution, if they are not clearly known, and ensures that the financial institution:
6.9.5. in the case of opening accounts, has conducted proper due diligence on the customers who are parties to the transactions carried out through those accounts, and may provide the necessary information regarding the due diligence on those customers upon request.

CHAPTER 7. QUALIFICATION OF A TRANSACTION OR BUSINESS RELATIONSHIP AS SUSPICIOUS, THEIR SUSPENSION, TERMINATION, OR REJECTION, FREEZING OF PROPERTY OF PERSONS RELATED TO TERRORISM AND THE PROCEDURE AND CONDITIONS FOR REPORTING TO THE AUTHORIZED BODY

7.1 A transaction may be qualified as suspicious both at the time of conducting the transaction (servicing the Customer) and during the ongoing due diligence monitoring of Customer transactions.
7.2 A transaction or business relationship, including an attempt to conduct a transaction or establish a business relationship, shall be qualified as suspicious and a report on the suspicious transaction or business relationship shall be provided 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 has been obtained through criminal means or is related to the financing of terrorism.
7.3 If the transaction or business relationship is not qualified as suspicious and a report on the suspicious transaction or business relationship is not provided to the Central Bank of Armenia, the justifications for not qualifying the transaction or business relationship as suspicious, the conclusions made, the analysis process and results thereof are documented and kept by the Company for at least 5 years unless a longer period is set by the Company's internal legal acts.
7.4 In cases where it is impossible to conduct proper customer due diligence, or the Company receives an instruction from the Authorized Body to reject or terminate the execution of a transaction or the establishment of a business relationship, the Company shall reject or terminate the execution of the transaction or the establishment of the business relationship and consider the issue of qualifying it as suspicious.
7.5 The Company has the right, in the case of suspicion of money laundering and/or financing of terrorism, or if it fails to form a real and complete picture of the Customer’s identification, transaction, business relationship and other specified information, or in cases of business

relationships or transactions matching the names (titles) or typologies presented by the Authorized Body, to suspend the business relationship or transaction for up to 5 (five) business days and submit a report on the suspicious transaction to the Authorized Body.
7.6 Monetary funds and securities directly or indirectly owned by or controlled by persons included in the lists published in accordance with the resolutions of the United Nations Security Council are subject to immediate freezing without prior notification of the said persons.
7.7 Freezing of the Customer's property may also be carried out on the basis of a decision of the Authorized Body.
7.8 In the case of making a decision on the freezing of securities or monetary funds of persons included in the lists provided for in this Chapter, the notification on the suspicious transaction/business relationship is immediately sent to the Authorized Body.
7.9 The implementation of the processes provided for in this Chapter on suspicious transactions/business relationships in the Company is carried out in compliance with the provisions stipulated in the "AML/CFT Procedure," the requirements of the Law, and the legal acts adopted based thereon.

CHAPTER 8. REQUIREMENTS FOR COMPLIANCE WITH INTERNATIONAL SANCTIONS

8.1 International sanctions (hereinafter referred to as the "Sanctions") are established through international legal acts adopted by international and intergovernmental organizations, international treaties concluded between countries, laws, and other legal acts adopted by state bodies of various countries, which are regularly monitored by the FMC.

8.2 The coordination of compliance with the requirements of international sanctions in the Company, their implementation and, if necessary, staff training thereon, and the introduction of tools and processes related to the issues, is carried out by the IMB.
8.3 When serving customers in the Company, interested subdivisions take measures to comply with the sanctions established by the UN, the USA, the EU, the United Kingdom, and, if necessary, other countries, relevant bodies of countries, international organizations, and intergovernmental organizations.
8.4 The Company follows and complies with the following types of Sanctions:
8.4.1 restrictions applied to countries,
8.4.2 restrictions applied to the types of goods and (or) spheres of activity of countries or territories,
8.4.3 restrictions applied to individuals, and
8.4.4 requirements for asset freezing.
8.5 The Company's employees shall carry out customer service while maintaining the approach applied by the Company regarding restrictions on countries, types of goods and/or spheres of activity of countries or territories.
8.6 The Company maintains the requirements of international sanctions in relations with customers, partners, and persons providing services to the Company, including correspondents, payment and settlement systems, suppliers, and all types of third parties.

8.7 The IMB, based on the approaches of partner organizations and the possible risks arising from international sanctions and accepted behavior in business practice, may propose to apply a stricter approach than the requirements of international sanctions if, in the opinion of the IMB, it is necessary to reduce reputational and financial risks.
8.8 Regardless of the position held, all employees of the Company are prohibited from assisting, showing inaction, transforming or concealing information, or providing advice to customers in order to avoid the requirements of international sanctions.
8.9 For checking coincidences of persons subject to international sanctions or listed by relevant authorities, the Company applies a software system and special information databases.
8.10 In order to make a final decision regarding transactions directly or indirectly related to or involving persons under international sanctions and/or included in the relevant lists, the IMB initiates a discussion with the participation of other interested persons designated by the Company's management bodies. The results of the discussion and the final decision on the execution of the transaction are subject to recording.
8.11 If international sanctions are applied to an existing customer or his/her transactions at any point, the Company shall apply the requirements established by international sanctions within a reasonable time frame, if necessary, terminating the business relationship with the customer and/or rejecting transactions, which is also carried out in accordance with the requirements of the current legislation. These provisions are also applicable in relations with the Company's partners, suppliers, and other cooperating persons.
8.12 For a transaction (business relationship) characterized by high-risk criteria for violating the requirements of international sanctions, the Company may decide to reject the transaction, attempt to establish a business relationship or terminate the existing business relationship with the customer. Moreover, for the purpose of making a final decision, at the initiative of the IMB, a discussion is organized with the participation of the BDD and, if necessary, other interested persons designated by the Company's management bodies. The results of the discussion and the final decision on the execution of the transaction are subject to recording.

CHAPTER 9. THE ROLE AND FUNCTIONS OF THE INTERNAL AUDITOR IN THE PROCESS OF COMBATING ML/TF AND COOPERATION WITH THE INTERNAL MONITORING BODY

9.1. In order to ensure a full level of three-tier control of the Company, the Internal Audit, in accordance with the procedure established by the Law, conducts inspections at least once a year to ensure that the Company's Executive Director and the Internal Monitoring Body ensure full compliance of the Company's activities with the requirements of the Law, normative legal acts of the Authorized Body, this Policy and other internal legal acts.
9.2. The Internal Audit submits a report to the General Meeting (a copy to the Executive Director) on its assessments and findings formed as a result of the inspections, including its conclusion on the adequacy and effectiveness of training and retraining of employees on ML/TF prevention issues.

9.3. If, during the current or planned inspection of any subdivision, the Internal Audit detects suspicious transactions or probable money laundering schemes, violations of requirements based on the Law and other legal acts adopted based thereon (internal and external), before submitting the document on the results of the inspection to the relevant competent authority, it shall inform the Internal Monitoring Body in order to implement the necessary measures to combat ML/TF.

CHAPTER 10. REPORTS PROVIDED BY THE INTERNAL MONITORING BODY TO THE GENERAL MEETING OF THE COMPANY AND THE PROCEDURE FOR THEIR SUBMISSION

10.1 The Internal Monitoring Body, at least once every six months, no later than day 30 of the month following the half-year (unless otherwise provided by the Company's internal legal acts and/or at the request of the General Meeting), prepares and submits to the General Meeting of the Company the reports established by the Law and internal legal acts.
10.2 The semi-annual regular report submitted by the Internal Monitoring Body to the General Meeting of the Company shall at least include:
1) the number of transactions subject to mandatory reporting,
2) the number and brief description of suspicious transactions (business relationships),
3) the number and summary description of transactions and business relationships that have been analyzed but not presented as suspicious transactions or business relationships,
4) the number and brief description of suspended or rejected business relationships and transactions,
5) the value of suspended transactions,
6) the amount of frozen financial resources,
7) other issues and information related to the fight against ML/TF, and
8) other information required by the General Meeting of the Company.

CHAPTER 11. TRAINING OF THE COMPANY'S EMPLOYEES ON ML/TF PREVENTION ISSUES

11.1 The Company organizes training for employees, including the management bodies of the Company and the Internal Audit, on the topics of combating ML/TF and maintaining international sanctions at least once a year, and for newly hired employees, within 3 months after employment.
11.2 The IMB develops and updates the training program every year, which shall include changes in the RA legislation in the field of ML/TF prevention, regulation aimed at maintaining international sanctions, information on the regulation introduced in the Company regarding the latter and changes thereof, as well as the training schedule is determined, which is submitted for approval to the Executive Body within the framework of the IMB's annual program.
11.3 The IMB may also organize separate thematic, special courses, tests, and discussions.
11.4 The training materials, the data of the employees who participated therein, and the documents confirming participation shall be recorded and stored for at least 5 (five) years unless a longer period is established by the Company's internal legal acts.

CHAPTER 12. PROCEDURE FOR COLLECTING AND STORING INFORMATION

12.1 The information specified by the Law and the Policy can be collected and stored in paper and/or electronic form.
12.2 The information required by the Law and the Policy, including the information obtained during the CDD, is stored in the Company, regardless of the circumstance of continuing or terminating the transaction or business relationship.
12.3 The information is collected in a separate package for each customer.
12.4 The Company stores the information required by the Law and the Policy, including the information obtained during the CDD, for at least 5 (five) years after the termination of the business relationship or after the execution of the transaction, and in the case of being established by the legislation or the Company's internal legal acts, for a longer period.
12.5 The Company's employees are prohibited from removing, reducing, and/or concealing any information about the customer and/or the transaction performed by him/her.

CHAPTER 13. RESPONSIBILITY FOR VIOLATION OF THE REQUIREMENTS OF THIS POLICY

13.1 Each management body of the Company is responsible for the proper and complete implementation of the functions assigned to it by the Law and this Policy, for organizing the elimination of obstacles to the effective organization of ML/TF prevention.
13.2 The head of each structural subdivision of the Company is responsible for properly organizing and ensuring the implementation of the functions and requirements established by this Policy in his/her subdivisions, and for promptly cooperating with the Internal Monitoring Body.
13.3 The Internal Monitoring Body is responsible for the proper and complete fulfillment of the functions and requirements established by the Law, the normative legal acts of the Authorized Body, and this Policy, for providing reports and other information to the Board of the Company, the Executive Director, and the Authorized Body.
13.4 The Executive Director, the heads of the Service Subdivisions, and the employees are responsible for violating the requirements of this Policy in accordance with the procedure established by the Law, the Company's internal legal acts, and/or by the decision of the competent authority.

CHAPTER 15. TRANSITIONAL PROVISIONS

15.1. The issues related to ML/TF prevention not regulated by this Policy are determined by the Law, the normative legal acts of the Authorized Body, and the internal legal acts of the Company's Internal Audit Activity Policy, regulations on the procedure, terms, and responsibility for submitting reports.

15.2. This Policy is approved and amended by the General Meeting, and the changes made thereto come into force from the moment of approval by the Board.
15.3. The Policy shall be reviewed at least once a year, as well as in the case of necessity to bring it in line with significant changes in the Law and the normative legal acts adopted based thereon. The drafts of this Policy and amendments thereto are developed and submitted for approval by the Internal Monitoring Body.
15.4. Within a week from the moment of approval of this Policy (changes and additions made thereto), it is submitted to the Authorized Body.

Appendix 1

CUBE INVEST CJSC Anti-Money Laundering and Counter-Terrorism Financing Policy

Table 1

ML/TF risk factors and characteristics of their relative importance, including circumstances of increased risk that require enhanced due diligence or application of restrictions.

	Description	**Risk Appetite**	**Commentary**
1.	Anonymous or fictitious name accounts	Prohibited	-
2.	Other accounts expressed solely through numerical, alphabetical, or other conventional symbols	Prohibited	-
3.	Securities by presenter	Prohibited	-
4.	Any business relationship with shell banks or with financial institutions that are known to permit their accounts to be used by shell banks	Prohibited	-
5.	Legal entities or individuals included in the FATF "blacklists,"[1] registered or operating in those countries, or individuals residing in those countries	Prohibited	-
6.	Individuals included in the OFAC, EU, and UK sanctions lists.	Prohibited	-
7.	Legal entities with 50% or more of their shares owned by shareholders who are on the OFAC, EU, and UK sanctions lists.	Prohibited	-
8.	Individuals and legal entities characterized as "sanctions-related persons" in publicly available reliable sources and widely used information databases (e.g., Worldcheck, Accuity), including: - Persons who have a direct connection with individuals and organizations included in the sanctions lists, such as family members of listed individuals, including spouses, children, parents, and, in the case of legal entities, owners, beneficial owners, and high-ranking officials within the legal entity's structure.[2]	Prohibited	-
9.	Individuals and legal entities involved in ML/FT and FPWMD crimes,	Prohibited	Including those suspected, accused, or convicted.

[1] https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-june-2024.html

[2] Board/Management/Executive Body Members

10.	Individuals and legal entities registered or operating in countries considered high-risk for FT and FPWMD.[3]	Prohibited/Restricted	Customer due diligence (CDD) may be applied to clients from these countries, and they may be served if there are reasonable explanations and documentary grounds confirming the presence of economic or other legitimate justifications for using the Armenian financial or non-financial system.
11.	Individuals registered in countries characterized by high corruption risks, residents of those countries, and those operating in sectors characterized by corruption risks (e.g., construction, pharmaceutical industry (narcotics), healthcare, arms trade, and mining).[4]	Limited/High Risk	A business relationship may be established only if, in addition to obtaining complete information required for CDD by legislation and the Company's internal legal acts, the account-opening company has and applies an anti-corruption policy, ML/FT, and sanctions prevention procedures, and is characterized as a leading reputable organization in the industry on the internet or in private information databases.
12.	Politically Exposed Persons (PEPs), their associated persons, and family members from countries characterized by high corruption risks.[5]	Prohibited/Restricted	Exceptions are made when, in addition to obtaining complete information required for CDD by legislation and the Company's internal legal acts, the source of income is clearly justified, the person's salary is compatible with his/her assets, and there is no negative information, particularly of a corrupt nature, in publicly available sources and private information databases regarding

[3] The list of countries is determined based on the list of countries identified by the Authorized Body within the framework of the national risk assessment for ML/FT and FPWMD.
Afghanistan, Jordan, Lebanon, Syria, Turkey, Iraq, Pakistan, Libya, Nigeria, Chad, Sudan, Yemen, Bangladesh, Mali, Somalia, Nigeria

[4] The list of countries characterized by high corruption risks is determined based on the "Corruption Perceptions Index 2023" report published by Transparency International (https://transparency.org.au/wp-content/uploads/2024/01/Report_CP2023_English.pdf). Countries with a score below 40 on the corresponding scale are considered high-risk.
Algeria, Angola, Benin, Bhutan, Botswana, British Virgin Islands, Burkina Faso, Cambodia, Cameroon, Cape Verde, Cayman Islands, Central African Republic, Chad, Republic of Côte d'Ivoire, Democratic Republic of the Congo, Denmark, Eswatini, Federal Democratic Republic of Ethiopia, Gabon, Gambia, Guinea, Guinea-Bissau, Haiti, Iceland, Kenya, Laos, Liberia, Madagascar, Mali, Mauritania, Mongolia, Mozambique, Myanmar, Nepal, Nigeria, Pakistan, Congo, Saint Kitts and Nevis, Saint Lucia, Senegal, Sierra Leone, Solomon Islands, Sri Lanka, Suriname, Tanzania, Togo, Tunisia, Turks and Caicos Islands, Uganda, Vanuatu, Venezuela, Vietnam, Zimbabwe.

[5] See the previous note.

			both the person and his/her associated persons and family members. In this regard, it is suggested that within the framework of the "Know Your Customer" process, it is necessary to obtain information about legal entities associated with the PEP and his/her family members.
13.	Trusts or similar legal arrangements, as well as legal entities with complex structures, which are registered, resident, or operate in countries with ineffective transparency and information exchange regimes.[6]	Prohibited	-
14.	Organizations operating without a license, if the legislation of the country of operation requires licensing for the relevant sector.	Prohibited	-
15.	Organizations engaged in adult entertainment.	Prohibited	-
16.	Organizations engaged in the sale and purchase of weapons	Prohibited	With the exception of the Ministry of Defense of the Republic of Armenia
17.	Individuals and legal entities investing in the cryptocurrency sector	High Risk	E.g., Contracts for Difference, where the client does not actually own the assets
18.	Embassies, consulates, and similar representations	High Risk	-
19.	Non-profit organizations, with the exception of organizations associated with countries at risk for FT	High Risk	-
20.	Organizations operating in the nuclear energy sector	High Risk	With the exception of companies under the supervision of the RA government agencies
21.	Legal entities operating in sectors characterized by corruption risks (construction, pharmaceutical industry (narcotics), healthcare, arms trade, mining) that are not associated with countries characterized by high corruption risks	High Risk	-
22.	Organizations characterized by extensive use of cash (including restaurants, retail stores, liquor stores, tobacco suppliers, etc.) that are not associated with countries with strategic deficiencies in ML/FT	High Risk	-
23.	High-net-worth individuals who have at least USD 1 million in highly liquid assets or cash	High Risk	-

[6] As countries with ineffective information exchange and transparency regimes, it is proposed to consider legal entities registered or operating in countries that have been simultaneously assessed as having a "Low" level of effectiveness in "Immediate Outcome 2 (International Cooperation)" and "Immediate Outcome 5 (Legal Persons and Arrangements)" according to the assessments of the FATF and FATF-style regional bodies, including trusts. The list of relevant countries is presented as of March 2024. (https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-ratings.html)

24.	Trusts and similar legal arrangements, as well as legal entities with complex structures (with the exception of legal entities and arrangements registered or operating in prohibited countries)	High Risk	-
25.	Organizations operating in the mining industry	High Risk/Restricted/Prohibited	There is a union of countries regarding transparency in this sector: Extractive Industries Transparency (EITI). Organizations that are residents of member countries can be classified as high risk, while others can be classified as restricted or prohibited, depending on the country's risk or the nature of the restriction set by the Company.
26.	Companies engaged in the extraction and processing of precious stones and metals	High Risk	
27.	Customers whose servicing, in the reasonable opinion of the Company's IOB and/or based on signals received from the Authorized Body, contains significant reputational risks, regardless of the risk appetite specified in this document.	High Risk/Restricted	

Table 2

Quantitive Criteria for Risk Appetite

	Description	Current Indicator	Risk Appetite	Deviations approved by the General Meeting	Commentary
1.	Proportion of non-residents in the total customer base	49%	55%	5%	Update data and reassess risk once a year
2.	Number of high-risk customers in the total customer base	17.2%	20%	3%	Update data and reassess risk once every 6 months

Including in high risk

3.	Proportion of high-risk individuals	54%	55%	3%	Present the customer base structure in the ML/FT report every quarter.
3.1	Proportion of PEPs/high-net-worth customers among high-risk individuals	58%	60%	3%	
4.	Proportion of high-risk legal entities	46%	45%	3%	
4.1	Proportion of high-risk financial institutions among high-risk legal entities	33%	35%	1%	
5.	Companies whose shareholder structure includes participants who are on the OFAC, EU, and UK sanctions lists and whose total share does not exceed 50%.	<0.5%	1%	1%	Provided that the company is able to conduct CDD on transactions of these customers.