UGURAS KIYMETLI MADENLER SANAYI VE DIS TICARET ANONIM SIRKETİ

COMPANY POLICY ON THE PREVENTION OF MONEY LAUNDERING AND THE FINANCING OF TERRORISM

1. INTRODUCTION

Within the scope of regulations established by the Financial Action Task Force (FATF), which was created to combat money laundering and the financing of terrorism at an international level, countries that are members of FATF are obliged to comply with these regulations and principles. As a member of FATF, our country ensures compliance with these international regulations through the Ministry of Treasury and Finance of the Republic of Turkey and the Financial Crimes Investigation Board (MASAK), which operates under it.

Accordingly, our Company has established this "Corporate Policy Document" in accordance with Law No. 5549, the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism, the Regulation on Compliance Programs Regarding Obligations Related to the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism, other relevant legislation, and the principles, standards, and guidelines issued by national and international institutions, provided that they do not conflict with the relevant legislation.

Within this framework, Uğuras Kıymetli Madenler undertakes to carry out its activities in compliance with:

- The Turkish Penal Code No. 5237,
- Law No. 5549 on the Prevention of Laundering Proceeds of Crime,
- The Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism,
- The Regulation on Compliance Programs Regarding Obligations Related to the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism,
- Law No. 6415 on the Prevention of the Financing of Terrorism,
- Law No. 7262 on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction,
- Responsible Gold Supply Chain Compliance Guides,
- And the recommendations, principles, standards, and guidelines published by national and international organizations.

2. PURPOSE

The purpose of this document is to ensure that our Company complies with the provisions set forth in **Law No. 5549 on the Prevention of Laundering Proceeds of Crime**, the relevant regulations and sub-regulations prepared based on this Law, and to fulfill its obligations on this matter by:

- Ensuring the compliance of the Company's policies, procedures, and control methods with the law and the regulations issued by the authorized institutions,
- Preventing the use of the Company's commercial activities for the purpose of money laundering and financing of terrorism,
- Evaluating customers, transactions, and services with a risk-based approach in order to eliminate risks the Company may face in this regard,
- Informing Company employees about the fight against proceeds of crime and their legal and administrative responsibilities,
- Defining internal audit and training activities.

3. LEGAL FRAMEWORK

The legal basis of our Company's policy on the prevention of money laundering consists of:

- **Law No. 5549** on the Prevention of Laundering Proceeds of Crime,
- **Law No. 6415** on the Prevention of the Financing of Terrorism,
- **Law No. 7262** on the Prevention of the Financing of the Proliferation of Weapons of Mass Destruction,
- and the regulations and communiqués issued based on these laws.

In addition to national legislation, our Company also considers the recommendations, principles, standards, and regulations set forth by international regulatory institutions in this field, provided they are not in conflict with national regulations.

The task of formulating the strategy for combating money laundering and terrorism financing, and developing applicable policies and legislation, is carried out by **MASAK** (Financial Crimes Investigation Board).

Established within the OECD in 1989 to enhance national legal systems in the fight against money laundering, harmonize regulations, strengthen the role of the financial system, and ensure ongoing cooperation between member countries, the **Financial Action Task Force (FATF)**—of which Turkey became a member in 1991—issues recommendations that are binding on member states.

According to Article 282 of the Turkish Penal Code No. 5237, any asset value obtained through the commission of an offense punishable by at least six months of imprisonment is considered **proceeds of crime (dirty money)**.

The crime of laundering is defined as any action taken to transfer assets obtained through criminal activities abroad, or to conceal their illegitimate origin, or to make them appear as though they were acquired through legal means.

Law No. 6415 regulates the financing of terrorism and provides the legal foundation for implementing:

- the **1999 International Convention for the Suppression of the Financing of Terrorism**,
- relevant decisions of the **United Nations Security Council**,
- the procedures and principles for **freezing assets** in efforts to combat terrorism and the financing of terrorism.

Similarly, **Law No. 7262** aims to implement measures for programs and activities (e.g., nuclear or ballistic missile programs) prohibited by **UN Security Council Resolutions**, and to prevent the financing of the proliferation of weapons of mass destruction. The procedures for freezing assets are structured in a way similar to Law No. 6415.

4. DEFINITIONS

- **Asset**: Money; tangible or intangible, movable or immovable assets that can be represented by monetary value; all rights and legal documents or instruments proving ownership of these assets.
- **Proceeds of Crime**: Any asset value derived from any type of criminal activity.
- **Laundering**: The act of transferring proceeds of crime abroad, concealing their illicit origin, or carrying out various transactions to make them appear as legally obtained.
- **Crime of Money Laundering**: The offense of conducting transactions involving assets derived from crimes punishable by imprisonment of one year or more, with the intent to transfer them abroad, to conceal their illegitimate origin, or to make them appear legitimate.
- **Financing of Terrorism**: Intentionally providing or collecting funds, or assets convertible to money, with the knowledge—whether in whole or in part—that they will be used to commit terrorist acts.
- **Risk**: The potential for financial or reputational harm to the Company or its employees due to the use of its services for money laundering or terrorist financing, or due to non-compliance with legal obligations.
- **Ultimate Beneficial Owner (UBO)**: The real person(s) who ultimately control the legal person or entity without legal personality on whose behalf a transaction is conducted, or who ultimately hold influence over the account or transaction.
- **MASAK (Financial Crimes Investigation Board)**: An entity under the Ministry of Treasury and Finance responsible for creating policies and regulations, collecting and analyzing information, conducting investigations, and sharing findings with relevant authorities to prevent and detect money laundering.

- **FATF (Financial Action Task Force)**: An organization established in 1989 by the G7 within the OECD to develop legal systems, harmonize regulations, strengthen financial systems, and ensure continuous cooperation among member countries to combat money laundering and terrorist financing.
- **Politically Exposed Person (PEP)**: Individuals entrusted with prominent public functions, including heads of state/government, senior politicians, senior government, judiciary, or military officials, senior executives of state-owned enterprises, and important political party officials—whether domestic or foreign—as well as their close relatives and associates.
- **Proceeds of Crime (Dirty Money)**: Money or assets that are not legally obtained and/or not taxed, particularly those stemming from crimes punishable by at least six months of imprisonment.
- **Suspicious Transaction**: Any transaction, or attempted transaction, conducted through or with the Company that raises suspicion that the assets involved were obtained illegally, are used for illegal purposes, or are connected with terrorism or terrorist financiers.
- **TF (Terrorist Financing)**: Providing or collecting funds for terrorists or terrorist organizations, knowingly or intentionally, regardless of whether the funds are linked to a specific terrorist act.
- **Compliance Officer**: A person appointed with sufficient authority and resources to ensure compliance with obligations imposed under Law No. 5549 and relevant legislation.
- **Digital Payment Channels**: Systems and platforms enabling the transfer of funds or securities using electronic tools during goods or services transactions.
- **Policy**: The Company's Anti-Money Laundering and Counter-Terrorism Financing Policy.
- **Ministry**: The Ministry of Treasury and Finance of the Republic of Turkey.
- **Company**: Uğuras Kıymetli Madenler Sanayi ve Dış Ticaret A.Ş.

5. AUTHORITIES AND RESPONSIBILITIES

Our Company and its employees are strictly prohibited from engaging in any actions or transactions that would constitute or facilitate money laundering in any form. Accordingly, employees must exercise due diligence and care in their relationships with customers to identify any risk of money laundering. Failure to do so may result in legal consequences, including fines and imprisonment, in accordance with applicable laws.

Board of Directors:

The Board of Directors holds the ultimate responsibility for ensuring that the Compliance Program is implemented effectively and comprehensively within the framework of this Policy. Within the scope of the Compliance Program, the Board of Directors is authorized and responsible for:

- Ensuring the Company's compliance with obligations related to the prevention of money laundering and terrorist financing,
- Approving the institutional policy,
- Appointing the MASAK Compliance Officer and Deputy Compliance Officer,
- Evaluating the results of risk management, monitoring and control, and internal audit activities, and ensuring that necessary measures are taken.

MASAK Compliance Officer:

The Compliance Officer is responsible for executing all duties assigned by the relevant legislation, as well as any additional tasks assigned by the Board of Directors or the authorized member(s) thereof. The Compliance Officer is authorized to access all necessary documents and information within the Company and its business partners and is empowered to take corrective measures and issue directives related to their field of responsibility.

The duties, powers, and responsibilities of the Compliance Officer and the Compliance Unit are clearly outlined in the “Compliance Unit and Officer Duties and Responsibilities Document” approved by the Board of Directors. Any updates to this document become effective upon the approval of the Board or its authorized member(s).

Deputy Compliance Officer:

In the absence of the MASAK Compliance Officer, the Deputy Compliance Officer is responsible for performing all related duties with the same authority.

6. RISK MANAGEMENT POLICY

The Risk Management Policy encompasses the measures and operational rules related to the implementation of the Company’s customer acceptance policy.

Purpose of Risk Management:

The objective is to ensure that risks associated with money laundering and terrorist financing to which the Company may be exposed are:

- Identified,
- Rated,

- Assessed,
- And mitigated through appropriate precautions.

The Company regularly reviews and updates its risk management policy in light of evolving conditions, national legislation, and the recommendations, principles, standards, and guidelines issued by international organizations.

Activities conducted within this scope are reported to the Board of Directors at regular intervals.

The risk management process also covers internal preventive measures and operational rules for **Know Your Customer (KYC)** practices in line with national and international regulations on anti-money laundering, particularly under the principle of "Know Your Customer."

The principles for customer identification outlined in Chapter 3 of the Regulation on Measures are implemented in full.

6.1 Principles Regarding Customer Identification

Our Company is obliged to identify real and legal person customers in terms of their social, financial, and personal details. To this end, it takes all necessary measures, particularly concerning identity information, including verifying the authenticity of such documentation.

Obtaining documents once from customers with whom a continuous business relationship is established is not considered sufficient. Customers are monitored according to their risk levels, their transactions are tracked, and any changes are followed closely.

- Customer accounts must be opened in the customer's real name or title. Anonymous names, pseudonyms, or aliases are not acceptable.
- If identity verification cannot be completed or sufficient information about the purpose of the business relationship cannot be obtained, the customer shall not be accepted, and the requested transaction will not be carried out.
- Legal persons or entities with unclear or unnecessarily complex ownership structures, or for whom the ultimate beneficial owner cannot be identified, will not be accepted as customers.
- In the interest of mutual transparency, trust, and open communication, individuals or entities that avoid completing customer information forms or provide misleading/unverifiable information shall not be accepted as customers.
- No customer relationship shall be established with persons or entities listed on the:
    - UN Consolidated Sanctions List,
    - OFAC Sanctions Lists,

- EU Consolidated Financial Sanctions List,
- UK Consolidated List of Financial Sanctions Targets or similar international or national sanction lists.

- Entities or persons directly or indirectly controlled by, acting on behalf of, or collecting funds for those on the above lists are treated under the same restrictions.
- Customer names are checked against globally recognized Politically Exposed Persons (PEP) lists. In the case of a match, enhanced due diligence measures are applied.
- If there is any doubt, information, or documentation indicating that a potential customer's assets were not legally acquired, no business relationship will be established.
- If the adequacy or accuracy of previously collected identification documents is in doubt, or if identity verification cannot be completed, the customer relationship is terminated.

6.2 Identification Methods

For Natural Persons:

When identifying real persons, the following details must be obtained:

- Name and surname
- Place and date of birth
- For Turkish citizens: mother's and father's names
- Nationality
- Turkish ID number (for Turkish citizens)
- Type and number of identity document
- Address and signature specimen
- If available: phone number, fax number, and email address
- Information on occupation and employer

For foreign individuals, identity verification must be based on:

- Passport,
- Residence permit, or
- Another identity document deemed acceptable by the Ministry.

For Legal Persons:

The following information must be collected:

- Legal entity name
- Trade registry number
- Tax identification number
- Field of activity
- Full address
- Telephone number
- If available: fax number and email address
- Name, surname, place and date of birth, nationality, type and number of identity document, and signature specimen of the person authorized to represent the entity

For Foreign Legal Entities:

The identification of foreign legal entities must include:

- Entity name
- Equivalent of trade registry number in the home country
- Tax ID number
- Business activity
- Full address
- Telephone number
- If available: fax number and email address
- Identification and authorization details of the representative, including name, surname, date of birth, nationality, ID type and number, and signature specimen

Associations and Foundations:

Identification of associations requires:

- Name of the association
- Purpose
- Registry number
- Full address
- Telephone number

- If available: fax number and email
- For the representative: full identification and contact details, including signature specimen, and for Turkish citizens, parent names and Turkish ID number

For foundations:

- Name and purpose
- Central registration number
- Contact details
- Full identification and contact info of the authorized representative, similar to the above

Unions and Confederations:

Must include:

- Name and purpose
- Registration number
- Address and contact details
- Identification and authorization details of the representative(s), including nationality and ID information, plus for Turkish citizens, parent names and national ID number

Political Parties:

Identification must include:

- Name of the relevant party unit
- Address and contact details
- Full identification of the authorized representative

Entities Without Legal Personality (e.g., Joint Ventures):

Must include:

- Name
- Address
- If available: phone, fax, and email
- Identification and authorization details of the representative, including for Turkish citizens: parents' names and Turkish ID number

6.3 Declaration of Acting on Behalf of Another and Identification of the Beneficial Owner

According to **Article 15 of Law No. 5549 on the Prevention of Laundering Proceeds of Crime**:

"In transactions requiring identity verification performed through or on behalf of liable institutions, any person acting on behalf of another must declare in writing whom they represent before conducting such transactions. Failure to do so is punishable by imprisonment from six months to one year or a judicial fine up to five thousand days."

In addition, **Article 17 of the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism** states that liable institutions must:

- Take the necessary precautions to determine whether someone is acting on behalf of another person and identify the real beneficiary of the transaction,
- Display visible notices at all service points reminding customers of their obligation to disclose if they are acting on behalf of another,
- Obtain a written declaration from customers when establishing a continuous business relationship, stating whether or not they are acting on behalf of another person.

6.4 Identification of the Beneficial Owner

Individuals entering into a business relationship with the Company, or the real or legal persons on whose behalf transactions are conducted, as well as those who ultimately control or have final influence over the accounts or transactions, are defined as **beneficial owners**.

Accordingly, the Company takes necessary measures to determine:

- Whether someone is acting on behalf of another, and
- Who the real beneficial owner of a transaction or relationship is.

When establishing a relationship with a legal entity, the Company is required to identify the real person shareholders who own **10% or more** of the entity.

If there is suspicion that the identified shareholder is not the actual beneficial owner, or if no real person holds 10% or more, the Company must take steps to identify those who ultimately control the legal entity.

The identified individual(s) will be accepted as the **beneficial owner(s)**. If the beneficial owner cannot be determined, then the **senior executive(s)** with the highest level of authority registered in the trade registry will be accepted as the beneficial owner(s).

Similar measures are taken to identify the real individuals who ultimately control unincorporated organizations. If no beneficial owner can be determined, the person(s) with the

highest level of executive authority within the organization will be accepted as the beneficial owner(s).

6.5 Compliance Officer and Compliance Unit

The **Compliance Officer** is responsible for ensuring compliance with obligations arising from Law No. 5549 and related regulations. The Compliance Officer is appointed by the **Board of Directors** and reports directly to it.

To effectively carry out their duties, the Compliance Officer is granted all necessary authority by the Board, including:

- Access to all relevant information,
- Cooperation with internal departments, and
- Authority to issue reports and directives.

The Compliance Officer operates as part of the **Compliance Unit**, and their responsibilities, powers, and duties are formally defined in internal documentation approved by the Board.

7. PAYMENTS AND ANTI-MONEY LAUNDERING (AML)

In line with our commitment to responsible financial practices, the Company applies the same rigorous **Anti-Money Laundering (AML)** standards to digital payment channels and related technological processes used in operations.

We acknowledge that digital transactions, while increasing efficiency and convenience, also present risks such as anonymity, rapid fund transfers, and cross-border complexities. To manage these risks, the Company has established a comprehensive framework for monitoring and controlling digital payments, which includes:

Know Your Customer (KYC) and Customer Due Diligence (CDD):

All customers and business partners using digital payment methods are subject to strict identity verification and monitoring processes.

Transaction Monitoring:

Digital payment activities are continuously monitored through automated systems capable of detecting suspicious patterns and flagging unusual behavior.

Risk-Based Approach:

For transactions or counterparties that pose a higher risk—especially in jurisdictions with weak AML controls—enhanced due diligence procedures are implemented.

Compliance with Global Standards:

Our AML procedures for digital payments align with the standards set by international regulatory bodies such as the **Financial Action Task Force (FATF)**.

Through these measures, the Company ensures that the use of digital payment technologies does not compromise ethical or lawful business practices.

8. RISK MANAGEMENT

Article 11 of the **Regulation on Compliance Programs Regarding Obligations Related to the Prevention of Laundering Proceeds of Crime and the Financing of Terrorism** defines the **Risk Management Policy**. It states:

"Liable institutions must establish a risk management policy that considers the size of their operations, transaction volume, and the nature of the services they provide."

Purpose of the Risk Management Policy:

The goal is to identify, classify, monitor, assess, and mitigate risks to which the liable institution may be exposed, and to establish internal measures—particularly regarding customer identification—at a minimum.

To prevent money launderers and terrorist financiers from conducting transactions through our Company and to enable proper suspicious transaction reporting, it is essential to strictly comply with the principles and procedures set forth in MASAK regulations and outlined in this document.

Failure to do so may expose the Company and its employees to the following risks:

Customer Risk:

Risk that a customer or a person acting on their behalf or account uses the Company to launder money or finance terrorism. The Company takes necessary measures to avoid being misused.

Legal Risk:

Intermediary institutions may face serious legal consequences—including revocation of operating licenses—if they fail to fulfill their AML obligations consistently.

Reputational Risk:

As institutions operate based on trust, public perception of a company's integrity and the trust of its customers are among its most valuable assets. Risk to reputation is managed through clearly defined procedures such as the **Monitoring and Control Procedure**, prepared by the MASAK Compliance Officer and the responsible internal control manager.

This procedure covers:

- Internal control framework and assignment of responsibilities

- Risk-based control methods
- Principles for transaction monitoring
- Reporting protocols
- Evaluation of control effectiveness and action plans for improvement
- Risk reduction and mitigation measures
- Procedures for detecting and reporting suspicious transactions, as outlined in the **Suspicious Transaction Detection and Reporting Procedure** prepared by the Compliance Officer.

9. MONITORING AND CONTROL OBLIGATION

The Company carries out monitoring and control activities by considering the nature of the transactions conducted by its customers.

Purpose:

To protect the Company against risks and to ensure that operations are conducted in continuous compliance with:

- Relevant laws,
- Regulations and communiqués issued under the law, and
- The Company's internal policies and procedures.

In this context, the following monitoring and control activities are conducted as required by legislation:

9.1 Monitoring and control of high-risk customers and transactions

Transactions involving customers or activities classified as high-risk are subject to enhanced scrutiny.

9.2 Monitoring and control of transactions with high-risk countries

Transactions involving jurisdictions identified as high-risk are specifically tracked and reviewed.

9.3 Monitoring and control of complex and unusual transactions

Transactions that are not consistent with the customer's known profile or business activities are closely monitored.

9.4 Monitoring connected transactions exceeding identification thresholds

Where multiple linked transactions collectively exceed the legal threshold for customer identification, a sampling method is used to monitor and control them.

9.5 Document verification and updating

Mandatory documents—either maintained electronically or in physical form—are reviewed, and any missing or outdated records are completed and updated as needed.

9.6 Ongoing monitoring of transaction consistency

The customer's transactions are continuously assessed against their business profile, risk level, and known sources of funds.

The Company has long gone beyond document-based customer verification. It also evaluates the:

- Compatibility of the documents with the company's capacity, credibility, and market activity,
- Consistency between the business owner and the company's characteristics,
- Appropriateness of personnel for the company's scale,
- And whether the actual beneficiary or transaction purpose aligns with ordinary business logic and market demand.

This includes evaluation of:

- Capital structure vs. transaction volume
- Market behavior and pricing (especially in gold and precious metals)
- Execution of transactions only by authorized individuals and confirmation through wet-signed documents
- Suspicion of speculative or contrary transactions in one-sided market conditions
- Ensuring that all partners and documents comply with OECD standards

As part of its operations, especially in gold trade, the Company maintains compliance with **OECD principles** and **LBMA/Borsa Istanbul** regulations, requiring documentation, verification, and registration of certificates and serial numbers in a traceable and regulated process.

10. ANTI-MONEY LAUNDERING AND COMPLIANCE POLICY

The Company adopts a **zero-tolerance** approach to the use of its services and operations for:

- Money laundering,
- Terrorist financing, or
- Any form of illegal commercial activity.

Whenever there is a reasonable suspicion of money laundering risk within the supply chain, the Company takes determined steps to investigate and, if necessary, intervene in such activities.

The Company is committed to:

- Supporting global efforts to eliminate financial crimes, and
- Maintaining the highest standards of integrity and compliance across all its business practices.

11. DETECTION AND REPORTING OF SUSPICIOUS TRANSACTIONS

- In accordance with Article 4 of Law No. 5549 on the Prevention of Laundering Proceeds of Crime and Article 27 of the Regulation on Measures, if any information, suspicion, or condition arises suggesting that an asset involved in a transaction carried out or attempted through the Company may have been obtained illegally, the transaction—regardless of the amount—must be reported to the Compliance Officer using a Suspicious Transaction Reporting Form within the time frame specified by the legislation.
- The Compliance Officer must conduct a necessary investigation and report the suspicious transaction to the Financial Crimes Investigation Board (MASAK) in accordance with applicable regulations.
- Confidentiality:
  Except for courts during trials and auditors authorized to inspect legal compliance, no one, including the parties to the transaction, may be informed about the suspicious transaction report.

- Legal Protection:
  According to Article 10 of Law No. 5549, the Company and its personnel cannot be held legally or criminally liable for filing a suspicious transaction report.

12. RESPONSIBLE SOURCING AND SUPPLY CHAIN INTEGRITY STATEMENT

The Company recognizes its critical role in promoting **transparency and ethical practices** throughout the precious metals supply chain.

As part of our ongoing commitment to **corporate responsibility**, robust systems have been implemented to identify and prevent any association with:

- The financing of armed conflict,
- Human rights violations,
- Money laundering,
- Terrorist financing, and
- Other illicit activities.

We work constructively with all our suppliers to ensure full compliance with our **Precious Metals Sourcing Policy**.

Our objective is to ensure that all materials sourced by the Company come from **responsible and ethical origins**, fully aligned with:

- Our core values, and
- International best practices.

13. TRAINING POLICY

The Company's training policy, which covers both employees and business partners, aims to enhance corporate culture and awareness regarding:

- Risks associated with money laundering and terrorist financing, and
- The Company's legal obligations, policies, procedures, and practices in this field.

The processes and systems related to training are determined by the **MASAK Compliance Officer** and the manager responsible for training, ensuring effective implementation.

The training procedure covers at a minimum the following topics:

- Concepts of money laundering and terrorist financing
- Stages, methods, and case studies related to money laundering

- National regulations on the prevention of money laundering and terrorist financing
- Risk areas
- The Company's internal policies and procedures
- International regulations and best practices in combating money laundering and terrorism financing
- Principles of customer identification (Know Your Customer)
- Procedures for reporting suspicious transactions
- Requirements for data retention and documentation
- Obligations to provide information and documents to authorities
- Sanctions for non-compliance with AML/CFT obligations

14. INTERNAL AUDIT POLICY

The internal audit activities are carried out within the scope of the Company's **Internal Audit Policy** to provide reasonable assurance to the **Board of Directors** regarding the effectiveness and adequacy of the Company's anti-money laundering (AML) and counter-terrorism financing (CFT) policies and practices.

The audit process evaluates:

- The effectiveness and efficiency of the Company's policies, procedures, risk management, monitoring, control, and training activities,
- Compliance of the Company's operations with the current legislation, internal policies, and procedures,
- Identified deficiencies, errors, or misconduct,
- Recommendations and preventive actions to avoid recurrence of such issues.

Findings and recommendations are reported to the **Board of Directors**, and related **action plans** are followed up accordingly.

A copy of the **Internal Audit Report** is also submitted to the **MASAK Compliance Officer**.

Relevant information and statistics about the audit activities are regularly maintained and reported to MASAK within the legal timeframe (10 working days) and requirements via the Compliance Officer.

15. RECORDKEEPING

Under **Article 6 of Law No. 5549** on the Prevention of Laundering Proceeds of Crime, the Company is obligated to report transactions that exceed the legal threshold amount—either executed directly or intermediated by the Company—to **MASAK**.

According to **Article 7** of the same Law, the Company must also provide, completely and accurately:

- Any requested information, documents, and records—regardless of format—
- All necessary access credentials or keys needed to retrieve and display this information to MASAK and authorized auditors.

All documents falling under anti-money laundering (AML) legislation must be:

- Retained for **ten (10) years** from the date of issuance (for documents),
- From the date of last entry (for ledgers and records),
- Or from the date of the last transaction or account closure (for identity documents).

These must be presented to the authorities upon request.

16. EFFECTIVENESS

This policy enters into force upon approval and signature by the **Board of Directors**.

Any subsequent updates or revisions to this Policy will also become effective upon the Board's approval and signature.

The **MASAK Compliance Officer** is authorized to prepare and implement procedures and instructions based on this Policy.

Business units may also create rules to effectively apply the legislation, provided that such rules:

- Do not conflict with this Policy or procedures prepared by the Compliance Officer, and
- Are approved by the Compliance Officer.

Such rules may be included in internal policy, procedure, or instruction documents of relevant departments.