

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

1. Foreword

KÂR Katılım Altın Rafinerisi A.Ş. (the “Company”) conducts all of its business processes in line with the principles of ethical values, transparency, accountability, and compliance with applicable legal regulations.

2. Introduction

While conducting its activities, the Company establishes, implements and maintains a control and compliance framework aligned with national legislation and relevant international standards on the prevention of money laundering and terrorist financing. Based on the risk-based approach, appropriate due diligence, monitoring and control mechanisms are applied to customers, suppliers, business partners and transactions.

This Policy sets out the Company’s fundamental approach, governance principles, areas of responsibility and control mechanisms to be implemented within the scope of anti-money laundering and counter-terrorist financing (“AML/CFT”). The Company requires all employees and relevant third parties to act in compliance with this Policy.

The Company believes that a strong compliance culture is not only essential for meeting regulatory expectations, but also constitutes one of the fundamental pillars of a sustainable, reliable, and responsible business model.

3. Purpose and Scope

The purpose of this Policy is to establish the fundamental principles, controls, and responsibilities to be implemented by KÂR Katılım Altın Rafinerisi A.Ş. in order to ensure compliance with national and international regulations regarding AML/CFT within the scope of its activities, effectively manage financial crime risks, and protect the Company’s reputation, operations, and stakeholders.

Through this Policy, the Company adopts a “risk-based approach” in combating:

- Money laundering,
- Terrorist financing,
- Sanctions violations,
- Proliferation financing related to weapons of mass destruction,
- Financial crimes related to corruption and bribery,
- Suspicious transactions and commercial activities.

This Policy applies to:

- All employees,
- Members of the Board of Directors,
- Senior management,
- Customers,
- Suppliers,
- Consultants,
- Representatives,
- Dealers and branches,
- Third-party assurance providers,
- Business partners.

This Policy applies across all areas in which the Company operates.

4. Definitions

Anti-Money Laundering (AML): Refers to the laws, regulations, controls, and processes designed to prevent, detect, and report activities involving the concealment, conversion, transfer, or use of proceeds derived from criminal activities.

Due Diligence: Refers to the risk-based review, verification, and assessment activities conducted regarding customers, suppliers, transactions, business partners, supply chains, and other related parties.

Enhanced Due Diligence (EDD): Refers to additional and more comprehensive review, verification, and monitoring measures applied to high-risk suppliers, counterparties, transactions, jurisdictions, or activities.

Natural Person: Refers to an individual acting on his/her own behalf.

Business Relationship: Refers to a continuous commercial or professional relationship between the Company and a customer, supplier, business partner or third party.

Politically Exposed Person (PEP): Refers to individuals who are or have been entrusted with prominent public functions, as well as their close associates and family members, as defined under applicable legislation and international standards.

Proliferation Financing: Refers to activities aimed at financing the development, acquisition, manufacture, possession, transportation, transfer or use of nuclear, chemical or biological weapons and related materials.

Customer Identification: Refers to the process of identifying and verifying the identity of the relevant party in accordance with applicable legislation before establishing a business relationship or carrying out a transaction requiring customer identification.

MASAK: Refers to the Financial Crimes Investigation Board of the Republic of Türkiye Ministry of Treasury and Finance.

Know Your Customer (KYC): Refers to control and verification processes aimed at understanding the identity, business activities, risk profile and transaction behavior of customers and relevant parties.

Ultimate Beneficial Owner (UBO): Refers to the natural person(s) who ultimately owns, controls, or benefits from a legal entity or arrangement, directly or indirectly.

Risk-Based Approach: Refers to the process of identifying, assessing, and mitigating AML/CFT risks proportionate to the nature, scale, complexity, and risk profile of the Company's activities, customers, suppliers, products, services, and geographical exposure.

Suspicious Transaction: Refers to any transaction, attempted transaction, or activity that may be related to money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, corruption, or other criminal conduct, or that lacks an apparent lawful or economic purpose.

Suspicious Transaction Report (STR): Refers to the report submitted to MASAK regarding suspicious transactions or activities following an assessment conducted within the scope of the applicable legislation.

Compliance Officer: Refers to the Internal Control and Supply Chain Compliance Officer responsible for managing, coordinating and monitoring the Company's AML/CFT compliance, risk management and control activities, including KYC and due diligence processes, sanctions and PEP screening, suspicious transaction assessment and reporting, training and awareness activities, and communication with relevant competent authorities where necessary.

Counter-Terrorist Financing (CTF): Refers to measures aimed at preventing, detecting, and reporting the provision, collection, transfer, or use of funds, assets, or other resources intended to support terrorist acts, terrorist organizations, or individual terrorists.

Sanctions: Refers to restrictive measures, prohibitions, embargoes, asset freezing decisions, or other limitations imposed by national or international authorities, including but not limited to the United Nations, the Republic of Türkiye, the European Union, the United States, or other competent authorities.

High-Risk Country / Region: Refers to countries or regions assessed by national or international authorities as presenting high risk in terms of AML/CFT, sanctions, corruption, regulatory deficiencies or weak supervisory mechanisms.

5. Legal Basis and References

This Policy has been prepared by taking into consideration the applicable national legislation, relevant international standards, and industry guidelines regarding the anti-money laundering, terrorist financing, and proliferation financing related to weapons of mass destruction.

The principal regulations and guidelines forming the basis of this Policy include the following:

- Law No. 5549 on the Prevention of Laundering Proceeds of Crime
- Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism (“**Measures Regulation**”)
- Regulation on Compliance Program Regarding Obligations on Prevention of Laundering Proceeds of Crime and Financing of Terrorism (to the extent applicable to the Company)
- Regulation on the Postponement of Transactions within the Scope of the Prevention of Laundering Proceeds of Crime and 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,
- Turkish Criminal Code (Law No. 5237)
- OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas
- LBMA Responsible Gold Guidance and Responsible Silver Guidance,
- Financial Action Task Force (FATF) Recommendations,
- The Strategy Document on Increasing Effectiveness in Combating Laundering of Proceeds of Crime and Financing of Terrorism and in Confiscation Practices in Türkiye (2026–2030), brought into force pursuant to Presidential Circular No. 2026/7 and published in the Official Gazette dated 4 July 2026 and numbered 33300
- Other recommendations, standards, and guidelines issued by national and international authorities and organizations.

6. Responsibilities

The Company adopts the principle of clearly defining the roles and responsibilities of all employees, governing bodies, and relevant business units in order to ensure the effective implementation of the control environment aimed at the AML/CFT.

6.1. Board of Directors

- Approving Company policies and control frameworks,
- Determining the Company’s risk appetite,

- Ensuring adequate resources and organizational structure for an effective AML/CFT compliance and control framework,
- Ensuring that the Internal Control and Supply Chain Compliance Officer reports to the Board of Directors at least monthly on AML/CFT, sanctions, PEP and adverse media matters, suspicious transaction assessments, high-risk customer/supplier relationships, critical compliance findings, training activities and corrective/preventive actions. Situations falling within the scope of critical / zero-tolerance cases, exact matches with sanctions or asset-freezing lists, significant findings that may be subject to suspicious transaction reporting, and matters that may require regulatory notification shall be escalated without delay to the Board of Directors or to senior management authorized by the Board of Directors. Reporting related to suspicious transaction reports shall be carried out in accordance with the confidentiality and non-disclosure provisions set out under the applicable legislation.
- Supporting and promoting a culture of compliance.
- To oversee that the Company's AML/CFT compliance and control framework is carried out in an adequate and effective manner, in line with the scope and risk profile of the Company's activities; to conduct the processes relating to the appointment of the Internal Control and Supply Chain Compliance Officer(s); to ensure that the duties, authorities and responsibilities of the relevant persons are determined in writing; to ensure the establishment of risk management, monitoring, control, training and, where necessary, internal audit or independent review activities; and to evaluate the results of such activities.

6.2. Senior Management

- Ensuring the operational implementation of Company policies,
- Supporting the effective integration of compliance, risk management, and internal control requirements into business processes,
- Operating the necessary escalation mechanisms for high-risk customers and transactions,
- Working in coordination with the Internal Control and Supply Chain Compliance Officer,
- Ensuring that corrective actions are implemented in cases of violations or deficiencies.

6.3. Internal Control and Supply Chain Compliance Officer (Compliance Officer)

- Ensuring the development, implementation, and sustainable monitoring of the Company's compliance, risk management, and internal control framework,
- Conducting Know Your Customer (KYC), sanctions screening, Politically Exposed Persons (PEP) checks, and due diligence processes,

- Managing suspicious transaction reporting processes,
- Monitoring regulatory developments and ensuring their integration into relevant processes,
- Conducting training and awareness activities,
- Coordinating communication with relevant regulatory and official authorities when necessary.

6.4. Finance and Accounting Department

- Executing payment flows in compliance with AML/CFT controls,
- Reviewing third-party payments and unusual financial activities,
- Ensuring the accuracy and traceability of records,
- Reporting suspicious financial activities to the Compliance Officer.

6.5. Human Resources

- Ensuring employee participation in internal Company training programs,
- Supporting appropriate ethical conduct and compliance awareness,
- Managing relevant disciplinary processes.

6.6. Employees

- Acting in compliance with Company policies and procedures,
- Promptly reporting suspicious situations to the Compliance Officer,
- Participating in mandatory training programs,
- Refraining from activities that violate Company policies, procedures, and control requirements,
- Providing requested information and documents accurately and in a timely manner.

6.7. Third Parties

- Acting in compliance with applicable legislation, regulatory requirements, and Company policies/procedures,
- Providing the information and documents requested within the scope of due diligence accurately, up-to-date, and in a complete manner,
- Complying with applicable national and international sanctions regimes, embargo regulations, and trade restrictions,
- Promptly notifying the Company of any suspicious transactions, unusual activities, or situations that may create compliance risks.

7. Risk Management

The Company shall conduct its AML/CFT activities within the framework of a risk-based approach. In this context, AML/CFT risk assessments shall be conducted

based on customers, suppliers, transactions, products, services, geographical regions, and business relationship models.

The Company's AML/CFT risk assessments, policies, procedures and control measures shall be established and updated by taking into account the current National Risk Assessment results, strategy documents, sectoral guidance and risk indicators issued by MASAK, findings of competent authorities, and findings arising from the Company's internal monitoring and control activities.

The Company applies risk-based review and verification processes regarding the origin, source of supply, supply chain route, and related commercial parties of precious metals. Precious metal transactions with unverifiable origin or those potentially linked to conflict-affected or high-risk areas shall be evaluated under enhanced due diligence procedures.

The Company shall apply enhanced due diligence measures for recycled precious metals and secondary material supply chains where origin verification risks, traceability concerns, or potential links to illicit activities are identified.

The identification and assessment of risks shall be carried out by the Compliance Officer. The classification of supplier, transaction, product, and location risks as low, medium, or high risk shall be conducted using the Risk Assessment Form annexed to the Company's Compliance, Risk Management and Internal Control Directive.

For high-risk customers, suppliers, business partners, transactions, products, countries/locations or supply chain-related risks, the applicable EDD, approval and escalation processes shall be carried out in accordance with the risk level, EDD triggers and approval/escalation principles set out in the Company's Compliance, Risk Management and Internal Control Directive and Risk Calculation, Assessment and Escalation Methodology. In very high-risk cases or in situations falling within the scope of critical / zero tolerance, the matter shall be reported to the Board of Directors and the necessary decision shall be taken by the Board of Directors.

The following factors shall be taken into consideration during risk assessments:

- Customer and supplier profile,
- Ultimate beneficial ownership structure,
- Countries and regions in which activities are conducted,
- Transaction volume and transaction patterns,
- Cash-intensive activities,
- High-value precious metal transactions,
- PEP relationships,
- Sanctions risk,
- Adverse media and reputational risk indicators,

- Complex or unusual transaction or supply structures.

The existence of the following factors in a risk assessment shall be considered as indicators of high risk:

- Countries and high-risk geographical regions with inadequate regulations or weak supervisory mechanisms regarding the AML/CFT, and sanctions enforcement,
- Transactions connected to offshore centers, free trade zones, and similar financial hubs that may pose risks related to illicit fund movements by providing banking secrecy, tax advantages, or limited transparency,
- Customers and third parties whose ultimate beneficial ownership structures are complex, non-transparent, or difficult to verify,
- Customers and third parties whose ultimate beneficial owners, shareholders, or senior executives include PEPs, family members of PEPs, or persons known to be close associates of PEPs,
- Transactions that are complex, unusually large, insufficiently explained in terms of economic purpose, or inconsistent with the customer profile,
- Transactions conducted through new or emerging technologies, payment methods, or digital tools that do not provide adequate transparency,
- Transaction requests that are inconsistent with the customer's business activities, financial profile, or historical transaction patterns,
- High-value precious metal transactions, cash-intensive activities, and cross-border fund movements,
- Precious metals whose origin, supply chain route, or actual source cannot be sufficiently verified, as well as transactions connected to conflict-affected and high-risk areas.
- Sectors that may carry high AML/CFT risk, such as precious metals trading, refining, recycling, logistics, and intermediary activities,
- Individuals and entities associated with sanctions lists, adverse media records, or regulatory investigations,
- Payment or delivery structures conducted through third parties without a clear commercial rationale.

Enhanced due diligence measures shall be applied for customers, suppliers, transactions, or business relationships assessed as high risk as a result of the risk rating process.

Within this scope, the following additional controls shall be implemented:

- Obtaining senior management approval,
- Verification of source of funds and source of wealth,
- Requesting additional documents and information,

- Conducting more frequent periodic reviews,
- Performing enhanced sanctions and adverse media screenings,
- Increasing transaction-based monitoring and control activities.

If the risk cannot be reduced to an acceptable level despite the additional measures taken, the Company shall not establish a business relationship, and shall suspend or terminate any existing business relationship.

Within the scope of its risk-based approach, the Company shall apply enhanced review and control measures in relation to high-risk countries, sectors, transactions and counterparties. The acceptance of high-risk customers, continuation of business relationships or execution of exceptional transactions shall be carried out in accordance with the risk level, EDD triggers and approval/escalation principles set out in the Company's Compliance, Risk Management and Internal Control Directive and Risk Calculation, Assessment and Escalation Methodology. In very high-risk cases, a Board of Directors decision shall be obtained; in critical / zero-tolerance situations, the matter shall be reported to the Board of Directors and necessary actions shall be implemented without delay.

Definitive matches with sanctions, asset-freezing or terrorism lists; suspicion of money laundering, terrorist financing or proliferation financing of weapons of mass destruction; sanctions evasion risk; submission of misleading or forged documents; concealment of the ultimate beneficial owner; intentional obstruction of compliance review processes; or links to bribery, corruption, smuggling, fraud or forgery shall be considered critical / zero-tolerance situations. In such cases, no business relationship shall be established; any existing business relationship shall be immediately suspended or terminated. The matter shall be reported by the Compliance Officer to senior management and the Board of Directors. Where necessary, notifications shall be made to MASAK, the Ministry, Borsa İstanbul or other competent authorities in accordance with the applicable legislation.

8. Know Your Customer (KYC) and Due Diligence Process

8.1. KYC and Due Diligence Principles

The Company shall implement risk-based Know Your Customer (KYC) and due diligence processes regarding customers, suppliers, business partners, and other relevant parties for the purpose of AML/CFT.

Where inconsistencies are identified between beneficial ownership information declared by the customer or relevant party and trade registry records, beneficial ownership declarations, share ledgers, ownership and control documents or other reliable sources, the Company shall request an explanation and supporting documentation. Where the inconsistency cannot be reasonably and verifiably

resolved, the business relationship and risk level shall be reassessed and the matter shall also be reviewed from a suspicious transaction reporting perspective.

Pursuant to Law No. 5549 and the customer identification and Know Your Customer provisions of the Measures Regulation, the Company performs customer identification before establishing a business relationship with natural or legal persons or before carrying out any transaction requiring customer identification. Customer identification is performed regardless of any amount threshold when establishing a permanent business relationship; where the transaction amount or the total amount of multiple linked transactions exceeds the monetary threshold prescribed under the applicable legislation; where a suspicious transaction report is required; and where there is doubt as to the adequacy or accuracy of previously obtained customer identification information.

Customer identification shall be completed before the establishment of the business relationship or before the execution of the relevant transaction. Within this scope, the monetary threshold of TRY 185,000 for transaction amounts or linked transactions shall be taken into account in accordance with the applicable legislation; where such threshold is amended by legislation, the current monetary threshold shall apply.

Before establishing a business relationship, the identity of the relevant party shall be verified, the nature of its activities and the purpose of the business relationship shall be assessed, and the ultimate beneficial owner shall be identified. The Company shall evaluate customers and transactions based on criteria such as customer profile, business activity, geographical risk, transaction structure, and sanctions risk.

When establishing a permanent business relationship with legal entities, the identity of natural person shareholders holding more than twenty-five percent (25%) of the shares of the legal entity shall be identified for the purpose of determining the ultimate beneficial owner. Where no natural person shareholder holding such percentage exists, or where there is doubt as to whether such persons are the ultimate beneficial owners, necessary measures shall be taken to identify the natural person or persons who ultimately control the legal entity. Where the ultimate beneficial owner cannot be identified in this manner, the natural person or persons holding the highest level of executive authority within the relevant legal entity shall be considered as the ultimate beneficial owner.

Enhanced due diligence measures may be applied for high-risk customers or transactions, and additional information, documentation, or senior management approval may be requested. In addition, sanctions list screenings, PEP checks, and adverse media controls shall be conducted.

Within this scope, necessary information and documents shall be obtained from natural and legal persons in accordance with applicable legislation, the risk-based approach and the Company's internal regulations.

For natural persons, identification information and necessary supporting documents shall be obtained in accordance with applicable legislation, the risk-based approach and the Company's internal regulations. This may include, but is not limited to, the following information:

- Full name
- Date of birth
- Nationality
- Type of identification document
- Identification number/passport information
- Occupation information
- Address information

For legal entities, necessary information and documents shall be obtained in accordance with applicable legislation, the risk-based approach and the Company's internal regulations, including but not limited to identification information, authorization documents, ownership structure information, and information and documents relating to the ultimate beneficial owner. This may include, but is not limited to, the following information and documents:

- Trade name
- Incorporation and business activity information
- Address
- Telephone number
- E-mail information
- Tax identification number
- Trade registry number
- Shareholder structure
- Authorized representatives
- Signature specimen

The Company shall conduct verification through independent and reliable data sources, official records, trade registry documents, licenses, operating permits, and other supporting documentation.

The Company keeps KYC information and documents relating to customers, suppliers, business partners and relevant third parties up to date in accordance with the risk-based approach. Identity, business activity, ownership structure, ultimate beneficial owner, authorized person, licence, permit, authorization and other KYC

documents of existing customers and suppliers are reviewed at least once every six (6) months.

Sanctions, asset-freezing, PEP, World-Check and adverse media/internet searches concerning customers, suppliers, ultimate beneficial owners, managers, authorized signatories, representatives and relevant supply chain actors identified based on the risk-based approach are renewed at least once every six (6) months. Country, origin, region and location assessments prepared on a customer/supplier basis are reviewed when necessary and, in any case, at least twice a year.

Controls relating to cash transactions, unusual payments and third-party payment risks are carried out on a monthly basis. The type, form, origin, source information, shipment and traceability records of the precious metal supplied are checked on a transaction-by-transaction basis.

Shorter control intervals may be determined for high-risk customers, suppliers, transactions or supply chains. Depending on the nature of the risk, monthly, transaction-based or event-driven enhanced monitoring may be applied. Where up-to-date information and documents cannot be provided or verified, or where the risk cannot be reduced to an acceptable level, the business relationship shall not be established; any existing business relationship shall be suspended, restricted or terminated.

8.2. Politically Exposed Persons (PEP) Controls

The Company conducts PEP checks for customers, suppliers, business partners, authorized representatives, ultimate beneficial owners, shareholders and senior executives within the framework of the risk-based approach. PEP screening is conducted as part of customer acceptance and KYC processes before establishing a business relationship; during the course of the business relationship, such screening is renewed periodically according to the risk level.

The identification of a person or relevant party as a PEP, a family member of a PEP, or a person known to be a close associate of a PEP does not, by itself, mean that the business relationship will be rejected. However, such status is considered a high-risk indicator and enhanced due diligence measures are applied where necessary. Within this scope, additional information and documents shall be requested, the source of funds and source of wealth shall be assessed, sanctions and adverse media screenings shall be enhanced, the purpose of the transaction and expected transaction profile shall be reviewed, and the establishment or continuation of the business relationship shall be subject to senior management approval.

Business relationships with parties identified as PEPs shall be reviewed more frequently, taking into account the nature of the business relationship, transaction

volume, country risk, business activity, source of funds and adverse media indicators. PEP screening results, risk assessments, approvals obtained and enhanced due diligence measures applied are recorded in the relevant customer/counterparty file and retained in accordance with the Company's record keeping principles.

9. Monitoring, Control and Audit Activities

The Company shall monitor and control its customers, transactions, and activities within the framework of a risk-based approach in order to identify, assess, and mitigate AML/CFT risks.

Transactions shall be evaluated based on criteria such as customer profile, transaction volume, transaction frequency, geographical risk, payment method, product/service type, and the purpose of the transaction. Unusual, complex, or economically or legally unjustified transactions may, where deemed necessary, be subject to detailed review.

Within the scope of monitoring and control activities, the following shall be assessed under a risk-based approach:

- Consistency of customer transactions with the customer profile,
- Connections to high-risk countries and individuals,
- Cash-intensive transactions,
- Fragmented transaction patterns,
- Risks related to the use of third parties,
- Sanctions and prohibited party controls,
- Unusual transaction behaviors

For payments and collections relating to the purchase, sale, supply, refining, delivery, return, service fees and similar precious-metals-related transactions, the Company shall, as a rule, use official banking channels through which party information can be verified and which provide traceability and documentary evidence. Cash payments or collections may be accepted only in exceptional circumstances permitted by applicable laws and regulations, provided that the purpose of the transaction, the source of funds, the amount and the justification are established through reliable and verifiable documentation, enhanced due diligence is applied, the transaction is assessed by the Internal Control and Supply Chain Compliance Officer, and written approval is obtained from the Board of Directors or senior management authorised by the Board of Directors. Where the risk cannot be mitigated to a reasonable level, the transaction shall not be carried out. The consistency between the account from which payment is made or to which funds are remitted and the customer or supplier that is party to the transaction shall be verified. Payments made from or directed to third-party accounts shall not be accepted unless assessed in advance by the

Internal Control and Supply Chain Compliance Officer and approved in writing by the Board of Directors or senior management authorised by the Board of Directors.

The Company documents findings identified through monitoring and control activities, conducts necessary reviews, and ensures that related processes are carried out in compliance with applicable legislation.

The effectiveness of monitoring and control processes is periodically reviewed by the Compliance Officer, taking into consideration risks and regulatory developments. Where necessary, independent assessment, review or consultancy support is obtained in order to evaluate the effectiveness of control processes.

The Company prepares an annual Responsible Supply Chain Compliance Report and is subject to independent assurance in order to assess the effectiveness of its responsible supply chain, AML/CFT and related compliance processes, within the scope of applicable legislation and regulatory requirements. The report and independent assurance outputs prepared within this scope are submitted to the relevant regulatory and competent authorities in accordance with the applicable legislation.

In addition, the Company regularly reviews the effectiveness of its AML/CFT, internal control and compliance processes within the framework of the legislation to which it is subject, regulatory requirements and the risk-based approach. Within this scope, internal control, internal audit or independent review activities may be carried out by taking into account the Company's organizational structure, scope of activities, transaction volume and risk profile. Such activities may be performed by the Internal Control and Supply Chain Compliance Officer, an authorized person/unit or, where necessary, independent service providers.

Within the scope of these activities, the effectiveness of risk management, monitoring and control activities, customer identification and due diligence processes, suspicious transaction assessments, sanctions and PEP controls, record keeping, training and reporting processes is evaluated. Identified deficiencies, errors, non-conformities or improvement areas are reported to the Board of Directors or authorized senior management, and necessary corrective/preventive actions are followed up.

Where any notification, reporting or information provision obligation arises towards MASAK, the Ministry, Borsa İstanbul or other competent authorities under the applicable legislation, such obligations are fulfilled within the prescribed procedures and time limits.

10. Prevention of Terrorist Financing and Proliferation Financing

The Company is committed to complying with applicable national and international regulations regarding the prevention of terrorist financing and the financing of the proliferation of weapons of mass destruction. Within this scope, the Company takes into consideration 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, relevant Financial Intelligence Unit (MASAK) regulations, and applicable United Nations Security Council resolutions.

The Company shall:

- Screen its customers, suppliers, business partners, and related ultimate beneficial owners against sanctions lists and relevant risk indicators,
- Comply with decisions and measures relating to asset freezing,
- Implement control mechanisms aimed at preventing direct or indirect business relationships with prohibited persons, entities, or countries,
- Assess, on a risk-based basis, transactions and activities that may give rise to risks of terrorist financing or proliferation financing.

In cases where circumstances arise requiring the implementation of an asset freezing decision within the Company, the necessary measures shall be implemented without delay in accordance with the applicable legislation and instructions of the competent authorities, and all legal notification obligations shall be duly fulfilled.

The Company shall not:

- Violate asset freezing decisions,
- Facilitate the circumvention of sanctions measures,
- Conduct any transaction that may result in the direct or indirect transfer of funds or resources to sanctioned persons or entities.

Where deemed necessary, the Compliance Officer is authorized to suspend transactions, request additional information and documentation, inform senior management, and make notifications to the relevant official authorities.

11. Suspicious Transaction Reporting

Company employees shall promptly report to the Internal Control and Supply Chain Compliance Officer any matter relating to customers, suppliers, business partners, transactions or activities that is suspected of being associated with money laundering, terrorist financing, sanctions violations, proliferation financing related to weapons of mass destruction or other related financial crimes, or that gives rise to suspicion.

Suspicious transaction assessments shall be conducted by the Internal Control and Supply Chain Compliance Officer by taking into consideration the customer's profile, line of business, transaction history, transaction structure and other relevant risk indicators. Where suspicion or reasonable grounds for suspicion arise, the suspicious transaction shall be reported to MASAK in accordance with the applicable legislation, regardless of the transaction amount. Suspicious transaction reports shall be submitted no later than ten (10) business days from the date on which the suspicion arises; in cases where delay may be prejudicial, the report shall be submitted immediately. Suspicious Transaction Reports to MASAK shall be made by the Internal Control and Supply Chain Compliance Officer in accordance with the powers and procedures prescribed under the applicable legislation. The ten (10) business-day deadline and the requirement for immediate reporting where delay may be prejudicial shall be applied by taking into account Law No. 5549, the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism, and Article 5 of MASAK General Communiqué No. 13.

Where the Compliance Officer is temporarily unable to perform their duties due to leave, illness or similar reasons, the Board of Directors shall, to the extent permitted by applicable legislation, promptly implement the necessary written delegation, authorisation and business continuity measures to ensure that suspicious transaction assessment and reporting processes continue without interruption and in compliance with applicable legislation.

Examples of suspicious transactions may include, but are not limited to:

- Transactions lacking an apparent economic or commercial rationale,
- Complex or unusual payment structures,
- Use of third-party accounts,
- Avoidance of identity disclosure,
- Connections with high-risk countries,
- Transaction patterns inconsistent with the customer's known business activities,
- Cash-intensive and fragmented transactions.

The Company shall report information relating to transactions subject to the continuous information provision obligation under Law No. 5549 and the relevant secondary legislation to MASAK, where such obligation arises, in accordance with the procedures, principles, format and time limits determined by the Ministry and/or MASAK. The submission of information within the scope of the continuous information provision obligation shall not eliminate the suspicious transaction reporting obligation. Where suspicion or reasonable grounds for suspicion exist, a

separate suspicious transaction assessment shall be conducted regardless of the transaction amount.

The Compliance Officer shall act in compliance with confidentiality obligations throughout the suspicious transaction review and reporting processes. Information and documents relating to suspicious transaction reports shall be retained in accordance with the applicable legislation.

Information regarding whether a suspicious transaction report has been made, will be made, or whether a review process is being conducted, shall not be disclosed to third parties, including customers, except where permitted under the applicable legislation.

12. Training and Awareness

The Company conducts regular training programs in order to enhance employees' knowledge and awareness regarding AML/CFT obligations. The Compliance Officer shall be responsible for the planning, implementation, and monitoring of the effectiveness of training activities.

Trainings shall be conducted regularly during the onboarding process and at least once annually thereafter. Training activities shall be reviewed, with the participation of relevant departments where necessary, based on assessment and evaluation results, and shall be repeated periodically in line with identified needs.

At a minimum, the training provided to employees shall cover the following subjects:

- a. Concepts of money laundering and terrorist financing,
- b. Stages and methods of money laundering, together with relevant case studies,
- c. Applicable legislation regarding the AML/CFT,
- d. Risk areas,
- e. Company policies and procedures,
- f. Within the framework of the Law and the relevant legislation,
 - Principles relating to customer identification and verification,
 - Principles relating to suspicious transaction reporting,
 - Record retention and submission obligations,
 - Information and document provision obligations,
 - Sanctions applicable in cases of non-compliance with obligations,
- g. International regulations and standards relating to combating money laundering and terrorist financing.

Training content shall be regularly updated in line with legislative amendments, emerging money laundering methods, sanctions-related risks, national and international regulatory expectations, and the Company's internal findings and experiences. Attendance records, training materials, measurement and evaluation

results, and other relevant documents relating to trainings shall be retained for at least eight (8) years.

Where necessary, the Company ensures the inclusion of external service providers and consultants in AML/CFT awareness activities.

13. Record Keeping and Confidentiality

The Company shall securely retain information and documents relating to customer identification, due diligence, transaction monitoring, sanctions screening, and suspicious transaction reviews conducted within the scope of AML/CFT obligations for a period of eight (8) years, as required under the applicable legislation.

The commencement date of the retention period shall be determined based on the date of issuance for documents, the date of the last entry for books and records, and the date of the last transaction for documents and records relating to customer identification, KYC/due diligence and customer/supplier identification processes.

Records shall be protected against unauthorized access, alteration, loss, or disclosure through appropriate physical and electronic controls. Customer information and documents obtained during due diligence processes shall be accessible only to authorized persons and shall be used in accordance with confidentiality principles.

The Company shall implement the necessary technical and administrative measures within the framework of personal data protection requirements, confidentiality of trade secrets, and other applicable legal obligations. The Company shall cooperate with competent authorities and institutions in accordance with the applicable legislation and shall fulfill its obligations relating to the provision of information, documents, records, and reporting in a timely, accurate, and complete manner.

14. Review and Update

This Policy shall be reviewed by the Compliance Officer at least annually, taking into consideration the applicable legislation, MASAK regulations, national and international sanctions regimes, industry practices, and the Company's activities and risk profile.

Where deemed necessary, the Policy may also be updated during the year in line with legislative amendments, audit findings, internal control results, risk assessments, organizational changes, or changes in the scope of activities. The Company shall be responsible for ensuring that the most current version of the Policy remains accessible.

15. Breaches and Sanctions

Any conduct contrary to this Policy, the Company's policies and procedures, ethical principles or applicable legislation shall be considered a breach. Taking into account the nature, severity, recurrence and impact of the breach, as well as the status of the relevant party, necessary administrative, disciplinary, contractual and/or legal actions shall be applied.

For employees, appropriate disciplinary and administrative actions shall be taken within the framework of applicable labour legislation, employment agreements, ethical principles and the relevant internal regulations of the Company. For third parties, suppliers, customers, business partners, service providers and consultants, necessary actions shall be applied within the framework of the relevant contractual provisions, undertakings and Company procedures, including the suspension, restriction or termination of the business relationship.

Depending on the nature of the breach and applicable legislation, notifications shall be made to competent authorities, reports shall be submitted to regulatory bodies or referrals shall be made to administrative/judicial authorities where necessary. The Company does not tolerate retaliation against persons who make reports in good faith.

In situations that give rise to, or may potentially give rise to, a conflict of interest, employees, managers, members of the Board of Directors and relevant parties acting on behalf of the Company are required to disclose such situation in a timely manner and in writing. Conflict of interest declarations shall be obtained at least annually and on an event-driven basis through the Conflict of Interest Declaration Form; declarations received shall be recorded, monitored and retained confidentially by the Internal Control and Supply Chain Compliance Officer in the Conflict of Interest Declaration Register.

16. Feedback

The Company values feedback and opinions from its stakeholders and maintains confidential grievance and whistleblowing mechanisms for the reporting of concerns, misconduct, or suspected violations. All concerns submitted to the Company are handled and evaluated in accordance with the principle of confidentiality. Concerns may also be raised anonymously. The Company strictly prohibits any form of retaliation, pressure, discrimination, or adverse treatment against any individual or party raising a concern in good faith. All reports submitted are reviewed and assessed by the Compliance Officer.

Questions, concerns, or feedback regarding this Policy may be submitted through the following channels:

Compliance Matters: compliance@karaltinrafinerisi.com

Ethics & Whistleblowing Notifications: etik@karaltinrafinerisi.com

Web Form: Ethics and Compliance Violations Reporting Form

Address: Yarımburgaz Mah. 1. Cumhuriyet Cad. No:50 İç Kapı No: 1 Küçükçekmece / İstanbul / TÜRKİYE

17. Publication and Transparency of the Policy

This Policy is published and made accessible to relevant stakeholders through the Company's official website and appropriate communication channels. The Company undertakes to keep the Policy publicly available, accessible, and up to date in line with the principle of transparency.

Related Documents:

- Precious Metals Responsible Supply Chain Policy
- Anti-Bribery and Anti-Corruption Policy
- Whistleblowing Policy
- Compliance, Risk Management and Internal Control Directive
- Annex-1 Risk Calculation, Assessment and Escalation Methodology
- Know Your Customer (KYC) Forms
- Personal Data Protection Notice
- Ethics and Compliance Violations Reporting Form
- Conflict of Interest Declaration Form
- Conflict of Interest Declaration Register

18. Approval and Effectiveness

This Policy was approved by the Board of Directors and became effective on 11/08/2026. In the event of any inconsistency, discrepancy or difference in interpretation between the Turkish version and the English version of this Policy, the Turkish version shall prevail.

Document Information	Description
Board Resolution Date	11/08/2026
Board Resolution Number	2026-05
Effective Date	11/08/2026
Version No.	01
Revision No.	00
Document ID	POL.25
Prepared By	Gökçe YILMAZ – Internal Control and Supply Chain Compliance Officer Şerafettin KULELİ – Internal Control and Supply Chain Compliance Officer
Approved By	Sercan YAŞA – Chairman
Last Review Date	07/08/2026
Next Review Date	19/07/2027
Publication Date	09.09.2026