

INFORMATION SECURITY POLICY

1. PURPOSE AND SCOPE

The purpose of this Policy is to establish the fundamental principles of KÂR Katılım Altın Rafinerisi A.Ş. ("the Company") regarding the protection of the confidentiality, integrity and availability of information assets owned by or entrusted to the Company.

This Policy aims to protect trade secrets, customer and supplier information, personal data, laboratory and production records, financial information and corporate systems through a risk-based approach.

This Policy applies to all information assets held in electronic, printed, verbal, visual or any other form, together with the persons, processes, applications, devices, networks, facilities and services that process such information assets.

Members of the Board of Directors, managers, employees, interns, consultants, contractors, suppliers and other parties granted access to information shall comply with the provisions of this Policy applicable to them.

2. FUNDAMENTAL PRINCIPLES AND OUR COMMITMENTS

The Company adopts and commits to the following principles in its information security management activities:

- To comply with applicable legislation, personal data protection obligations, contractual requirements and the information security requirements adopted by the Company.
- To establish, implement, maintain and continually improve the information security management system certified to ISO/IEC 27001:2022 through a risk-based approach.
- To maintain an inventory of information assets, assign asset owners, classify information assets according to their sensitivity and business value, and define appropriate handling rules.
- To grant access rights in accordance with the need-to-know and least-privilege principles, and to update or revoke access rights in a timely manner following changes in duties or the termination of employment or engagement.
- To implement authentication, privileged access, logging, network security, malware protection, secure configuration, patch management and vulnerability management controls in proportion to the relevant risks.
- To apply appropriate technical and administrative safeguards when sensitive information is transmitted, stored, copied, shared, physically transported or destroyed.

- To ensure the integrity of laboratory results, production and traceability records, and financial and commercial data against unauthorised alteration, as well as their availability throughout the applicable retention period.
- To manage the risk of disruption to critical processes through backup arrangements, restoration testing, business continuity and disaster recovery measures.
- To report, classify and respond to information security incidents, preserve relevant evidence, mitigate their effects and implement actions to prevent recurrence.
- To assess information security risks arising from suppliers, cloud services, software, infrastructure and outsourced services during selection, contracting, access management and performance-monitoring processes.
- To protect physical areas, server and network equipment, archives and critical working environments against unauthorised access, damage and environmental threats.
- To develop employees' awareness of information security and personal data protection during onboarding and through regular training, and to raise awareness of social engineering and similar threats.

3. DUTIES AND RESPONSIBILITIES

- The Board of Directors approves the Policy and provides oversight of information security risks.
- General Management provides the resources and authorities necessary for the information security management system and ensures that risk acceptance and critical improvement decisions are addressed at the appropriate level.
- The function responsible for information technologies and information security operates the relevant technical controls, coordinates risk assessments and incident response activities, and reports relevant records and performance indicators.
- Information asset owners are responsible for determining the classification, access requirements, retention needs and appropriate use of the information under their responsibility.
- Functions that process personal data comply with the principles of data minimisation and purpose limitation, as well as applicable retention and destruction requirements, and report any suspected personal data breach without delay.
- All users protect the access credentials and tools assigned to them, refrain from unauthorised sharing and report suspicious incidents through the designated channels.

4. MONITORING, RECORD-KEEPING AND FEEDBACK

4.1. Monitoring and Record-Keeping

- Information security performance is monitored through information security incidents, access reviews, vulnerability and patching status, backup and restoration tests, training activities, supplier controls and corrective actions.
- Risk assessments, internal controls, independent testing and management reviews are conducted according to the relevant risks and needs.
- Information security incident records and evidence are retained in accordance with applicable legislation and retention requirements, while preserving their confidentiality and integrity.

4.2. Feedback

Reports involving suspected ethical violations or nonconformities, as well as questions, concerns or feedback regarding this Policy, may be submitted through the following communication channels:

Ethics and Whistleblowing Reports: 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

Reports are assessed in accordance with the principles of confidentiality, impartiality, personal data protection and protection against retaliation. No adverse action against any person who makes a report in good faith shall be permitted.

5. BREACHES AND SANCTIONS

Conduct contrary to this Policy, the Company's policies and procedures, ethical principles or applicable legislation shall be deemed a breach. Necessary administrative, disciplinary, contractual and/or legal action shall be taken by considering the nature, severity, recurrence and impact of the breach and the status of the relevant party.

For employees, appropriate disciplinary and administrative action shall be taken in accordance with applicable labour legislation, employment contracts, ethical principles and relevant internal Company rules. For third parties, suppliers, customers, business partners, service providers and consultants, necessary action, including suspension, restriction or termination of the business relationship, shall be taken in accordance with the relevant contractual provisions, commitments and Company procedures.

Depending on the nature of the breach and the applicable legislation, the competent authorities shall be notified, regulatory reports shall be submitted or judicial/administrative authorities shall be contacted where necessary. The Company shall not tolerate retaliation against any person who reports a concern 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.

6. 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. In line with the principle of transparency, the Company undertakes to keep the Policy publicly available, accessible and up to date.

Related Documents:

- Personal Data Protection Notice
- Ethics and Compliance Violations Reporting Form
- Conflict of Interest Declaration Form
- Conflict of Interest Declaration Register

7. APPROVAL AND EFFECTIVENESS

This Policy was approved by the Board of Directors on 11/08/2026 and entered into force on the same date.

The Policy is reviewed by the responsible function at least once a year and additionally whenever there is a material change in applicable legislation, standards, the organisational structure, activities or the Company's risk profile.

In the event of any inconsistency, conflict or difference in interpretation between the English translation of this Policy and the Turkish text, the Turkish text 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.01
Prepared By	Gökçe YILMAZ – Internal Control and Supply Chain Compliance Officer Şerafettin KULELİ – Integrated Management System Representative Nurullah KARABİBER – ISO Management Systems Consultant
Approved By	Sercan YAŞA – Chairman
Last Review Date	07/08/2026
Next Review Date	02/08/2027
Publication Date	09/09/2026