



**KOCAER STEEL
INFORMATION SECURITY AND
INFORMATION SYSTEMS MANAGEMENT POLICY**



At Kocaer Steel, we believe that information security and reliable information systems are fundamental to our operational continuity, our corporate reputation, the trust of our customers and stakeholders, and our sustainable growth.

Our objective is to protect the confidentiality, integrity and availability of our information assets, to manage our information systems securely and in compliance with legislation, and to continuously strengthen our corporate cyber resilience against evolving cyber threats.

This policy covers the information assets and information systems at our headquarters, facilities, branches, affiliates and subsidiaries; our employees, executives, interns and consultants; and third parties that access our systems or process information on our behalf.

In line with this approach, we commit to:

- **Confidentiality, Integrity and Availability:** Protecting our digital and physical information assets against unauthorized access, alteration, loss and disclosure; ensuring availability in line with business needs; and protecting the personal data we process, our trade secrets and our intellectual property, including R&D data;
- **Risk-Based Management:** Assessing information security risks at least once a year and whenever significant system changes occur; determining risk acceptance and treatment decisions with the approval of senior management; and planning and monitoring improvement activities with defined resources and timelines;
- **Governance and Resource Allocation:** Defining responsibilities in accordance with the principle of segregation of duties, under the oversight of our Board of Directors, exercised through the Early Detection of Risk Committee and the Audit Committee, and the leadership of our senior management; ensuring coordination between the Information Security Committee and the relevant units; reviewing responsibilities at least once a year and allocating adequate budget, human resources and technology; and reporting our cybersecurity posture and the notifications made to regulatory authorities to our Board of Directors at least once a year;
- **Independent Oversight and Accountability:** Appointing an Information Security Officer with the technical competence required by legislation and at least five years of relevant experience; and ensuring that this role reports to senior management and does not conflict with operational duties related to the management of information systems;

- **Information Systems Strategy and Critical Projects:** Developing our information systems strategy in alignment with the Company's objectives; and implementing critical system projects and significant changes with the approval of senior management, after assessing their risks;
- **Asset Management and Classification:** Keeping the inventory of our information assets and systems, their owners and their dependencies on critical business processes up to date; and classifying information assets by criticality and sensitivity, taking into account confidentiality, integrity and availability requirements, and applying appropriate protection measures and handling and retention controls for each classification level;
- **Audit and Technical Verification:** Assessing our information systems and security controls at least once a year through internal audits and penetration tests conducted by authorized, independent organizations; subjecting our ISMS to an external audit by an accredited certification body under ISO/IEC 27001 at least once a year; and establishing improvement plans approved by senior management for the findings, implementing the necessary technical and administrative measures, and reporting the results to our Board of Directors;
- **Identity and Access Management:** Applying the principles of role-based access and least privilege; implementing strong authentication methods and establishing secure password standards; using multi-factor authentication for critical systems and privileged accounts; and reviewing access rights at least once a year and upon a change of role or termination of employment, removing unnecessary access;
- **Network and System Security:** Protecting our networks, systems and devices through a layered security approach; and logically segregating the industrial control and MES systems in our plants from office networks, limiting access to what the work requires;
- **Physical and Environmental Security:** Ensuring the physical and environmental security of our data centers and server rooms; and putting in place access control, fire detection and suppression, uninterruptible power supply, air conditioning and environmental monitoring measures, regularly auditing their effectiveness and continuity;

- **Incident Management and Timely Notification:** Establishing response plans for security incidents and vulnerabilities; ensuring that our employees and relevant third parties report suspicious situations promptly through defined channels; enabling information security breaches and suspected breaches to be reported through the Ethics Hotline as well; recording incidents, evaluating them at least once a year and eliminating their root causes to prevent recurrence; and notifying cyber incidents and vulnerabilities to the Directorate of Cyber Security without delay, and to the Capital Markets Board of Türkiye, the Personal Data Protection Authority and other relevant parties within the time limits prescribed by legislation;
- **Cooperation with Regulatory Authorities:** Responding to requests for information, documents and audits from the Directorate of Cyber Security and other competent authorities through a single channel, in a timely and complete manner; keeping our information systems open to authorized audits; and, should the Company be designated as critical infrastructure, fulfilling the additional obligations arising from that status;
- **Supplier and Outsourced Service Security:** Overseeing the risks and security compliance of externally provided information system services, including cloud services; securing confidentiality, service continuity, data protection, service termination and, where applicable, audit access provisions in contracts; procuring cybersecurity products and services from providers authorized by the Directorate of Cyber Security where required by legislation; and periodically auditing the compliance of suppliers and outsourced service providers with their information security obligations, as well as their performance;
- **Business Continuity and Recovery:** Defining acceptable downtime and data loss targets for critical information systems; preparing continuity, backup and recovery plans, testing and updating them at least once a year; and ensuring the timely resumption of priority activities in the event of a disruption;
- **Training and Security Culture:** Providing our employees with information security training appropriate to their roles and responsibilities at least once a year; strengthening awareness in units that work with R&D, personal data and trade secrets; and embedding secure working habits in our corporate culture;
- **Logging and Audit Trails:** Generating logs of critical transactions and access, protecting their integrity and security, and retaining them for the applicable retention periods; and regularly monitoring unusual activity and taking the necessary measures;

- **Regulatory Compliance and Responsible Conduct:** Complying with Cybersecurity Law No. 7545 and the regulations of the Directorate of Cyber Security, the Capital Markets Board of Türkiye's Communiqué on the Procedures and Principles Regarding Information Systems Management (VII-128.10), Personal Data Protection Law No. 6698, other regulations applicable to the Company and our contractual obligations; and evaluating breaches within the framework of legislation, internal regulations and contracts, ensuring that the relevant disciplinary, legal and contractual sanctions are applied where necessary;
- **ISMS Effectiveness and Continual Improvement:** Meeting the requirements of our Information Security Management System within the ISO/IEC 27001 framework and continually improving its effectiveness; and setting measurable objectives, monitoring control results and following up on improvement activities.

This policy is implemented with the approval of our Board of Directors, the oversight of our senior management, the participation of all our employees and the fulfillment of responsibilities by the relevant parties. We review the policy at least once a year and whenever significant legislative changes occur; submit revisions to our Board of Directors for approval upon the evaluation and recommendation of the Corporate Governance Committee; and communicate it to our employees and relevant parties.