



KOCAER STEEL
ARTIFICIAL INTELLIGENCE POLICY



At Kocaer Steel, we believe that artificial intelligence offers significant opportunities in terms of efficiency, quality and decision quality, and that these opportunities can only be turned into lasting value through a **secure, controlled and responsible approach to management.**

Our objective is to go beyond being a company that uses artificial intelligence and to become a company that manages artificial intelligence in a secure, controlled and value-driven way.

This policy covers all units of the Company and every artificial intelligence tool, agent and solution used or planned to be used in these units. It also covers the use of publicly available artificial intelligence tools with corporate data, the development and operation of in-house solutions, artificial intelligence features embedded in purchased software, and the related supplier relationships.

In line with this approach, we commit to:

- **Value-Driven Use:** Selecting artificial intelligence applications on the basis of business needs and measurable benefits; and scaling them up after evaluating their contribution to efficiency, quality, workplace safety and decision quality;
- **Risk-Based Assessment and Approval:** Subjecting every use of artificial intelligence to risk classification according to its potential impact on people, data and processes; and not scaling up any solution without approval proportionate to its level of risk;
- **Human Oversight and Accountability:** Always keeping final decision-making responsibility with people and using artificial intelligence as a decision-support tool; and not allowing artificial intelligence to make decisions on its own in processes that directly affect our employees, such as recruitment, performance appraisal and disciplinary matters;
- **Data Security and Privacy:** Not using any unclassified data in artificial intelligence systems; not transferring confidential, critical or personal data to publicly available artificial intelligence platforms, and processing such data only on approved and secure corporate infrastructure; and complying with personal data protection legislation and the requirements of our Information Security Management System;
- **Transparency and Traceability:** Conducting the corporate use of artificial intelligence transparently; keeping the solutions in use under an inventory, generating access and usage logs, and providing corporate access through centralized and auditable channels;
- **Accuracy and Reliability:** Verifying artificial intelligence outputs in a manner appropriate to their intended use; and monitoring solutions before deployment and throughout their use to prevent erroneous, misleading or discriminatory results;

- **Purchased Solutions and Suppliers:** Also evaluating the artificial intelligence features embedded in the software we purchase within the scope of this policy; and clearly setting out the terms of artificial intelligence use and data processing in our contracts with suppliers;
- **Incident Management:** Rapidly detecting and managing, through defined reporting channels, artificial intelligence incidents that result in erroneous or misleading outputs, data leaks or regulatory violations, and eliminating their causes to prevent recurrence; and making the legal notifications related to such incidents in accordance with the principles set out in our Information Security Policy;
- **Integration with R&D and Innovation:** Developing corporate artificial intelligence solutions in an integrated manner with our R&D and innovation activities; and benefiting from collaborations with universities, technology development zones and support programs;
- **Competence and Shared Responsibility:** Regarding the management of artificial intelligence as the shared responsibility of the entire organization rather than of the information technology unit alone; and developing our employees' artificial intelligence literacy and competencies through training;
- **Compliance and Sanctions:** Monitoring and complying with national and international regulations on artificial intelligence and the provisions of Personal Data Protection Law No. 6698 and Cybersecurity Law No. 7545 that apply to artificial intelligence systems; and evaluating conduct contrary to the policy, such as the unauthorized use of confidential, critical or personal data and the use of unapproved artificial intelligence tools, within the framework of our disciplinary processes.

We see artificial intelligence not as a substitute for human capability, but as a tool that strengthens it.

This policy enters into force upon the proposal of our General Manager, the favorable opinion of our Corporate Governance Committee and the approval of our Board of Directors. Our Board of Directors sets the vision and risk appetite for the use of artificial intelligence and oversees its implementation; the Artificial Intelligence Steering Committee, chaired by our General Manager, makes prioritization and risk acceptance decisions; and the Artificial Intelligence Office coordinates the implementation of the policy. We review the policy through the Artificial Intelligence Office at least once a year and whenever significant regulatory or technological changes occur; submit revisions to our Board of Directors for approval upon the evaluation and recommendation of our Corporate Governance Committee, also obtaining the opinion of our Early Detection of Risk Committee for changes affecting risk appetite; and communicate the policy to our employees and business partners and share it with the public on our corporate website.