INFORMATION SECURITY POLICY

Çolakoğlu® Metalurji A.Ş. commits to taking all necessary steps for the implementation, operation, continuous monitoring, review, maintenance, and improvement of information security. Information security is the responsibility of all employees and is an integral part of our corporate culture.

Information security is achieved by ensuring the confidentiality, integrity, and availability of information assets:

- Confidentiality: Ensuring that information is accessible only to authorized persons,
- Integrity: Protecting the accuracy and completeness of information and safeguarding it against unauthorized changes,
- Availability**:** Ensuring that information is usable by authorized persons whenever needed.

Çolakoğlu® Metalurji A.Ş. determines information security objectives, regularly monitors and measures compliance with these objectives; applies, executes, and continuously improves the management system in line with a risk-based thinking approach. It ensures compliance with relevant standards by performing necessary information security controls within the scope of Operational Technologies (OT) and commits to complying with current legal regulations and standards regarding power generation activities. It ensures full compliance with legal, regulatory, and contractual requirements; guarantees that the products and services offered meet the expectations of customers and stakeholders and ensures the protection of customer information. Taking into account the needs and expectations of internal and external stakeholders, it aims to protect the security of business processes and the continuity of production.

Adhering to the principles stated above, Çolakoğlu Metalurji aims to carry out its information security activities in line with the following objectives:

- The Information Security Management System ("ISMS") is planned, implemented, and developed in accordance with internationally recognized standards.
- ISMS objectives are determined periodically within the framework of the policy. The effectiveness of the system, the level of achievement of objectives, and the risk status are periodically reported to senior management. Management takes strategic decisions in line with the reports and allocates the necessary resources.
- Steps required for internal audits, management reviews, corrective actions, and the determination of risks and opportunities for the continuous improvement of the ISMS are provided by the management and the teams authorized by the management for information security. All roles and responsibilities related to information security are defined, and authorizations are made by the management.
- Resources and guidance for the execution of necessary work within the framework of the ISMS are provided by the management.
- Regular training and awareness activities are carried out to maintain the competencies of all employees and their commitment to management systems. By creating an open and transparent communication environment, the participation of employees in the continuous improvement of the system is ensured in line with their knowledge and experience.
- To manage all information security risks, including the Operational Technology (OT) and Industrial Control Systems (ICS) used in our organization's power generation facilities, risk assessment, risk analysis, and risk treatment activities are carried out; necessary measures are developed, and actions are taken to prevent potential risks.
- Together with its stakeholders, financial and moral losses that may negatively affect the competitive advantage of the organization are prevented.
- Within the scope of the ISMS, information assets are identified; information security expectations of interested parties such as customers, suppliers, and business partners are evaluated; and legal and contractual obligations are assessed.

- The organization commits to complying with all legal, regulatory, and contractual requirements related to the ISMS. Information security requirements, confidentiality provisions, data protection, and breach notification obligations are clearly defined in all contracts. Integration of information security controls is ensured in agreements made with third parties.
- Necessary work is carried out to reduce the probability of experiencing an information security breach incident; in the event of an incident, a coordinated response is provided.
- The organization establishes, implements, and tests Cyber Incident Response Team (CIRT/SOME) plans against information security breaches.
- All information systems, devices, and network components are securely configured and managed in line with security standards and best practices determined by the organization to minimize unauthorized access, privilege escalation, and security vulnerabilities. Critical security patches and updates are applied regularly.
- To manage risks within the scope of the ISMS, risk assessment, risk analysis, and risk treatment activities are performed, and work is carried out to implement necessary measures and prevent potential risks.
- Unauthorized access to all information of customers and stakeholders, including personal data, is prevented. Necessary efforts are made to ensure compliance with relevant laws and regulations, including the Law on the Protection of Personal Data (KVKK).
- Security assessments are performed from an information security perspective before the deployment of new technologies.
- By managing the ISMS effectively, damages that may arise from information security are minimized.
- Necessary arrangements are made to prevent interruptions in critical business processes; in cases where they cannot be prevented, it is ensured that they become operational within the targeted recovery time.
- Within the scope of the ISMS, the confidentiality, integrity, and availability of our customers' information assets are ensured.
- It is ensured that the change processes addressed within the ISMS are operated throughout their life cycle.
- The success of management systems in achieving intended results is reviewed periodically, and it is guaranteed that necessary improvements are implemented in a timely manner.
- The organization attaches importance to ensuring the security of its activities related to the products and services offered to its customers and stakeholders, aiming for them to be integrated, compatible, and balanced with business processes.
- An integrated and dynamic business strategy necessitates the security and continuity of information assets.
- Necessary measures are taken to ensure security in internal working areas such as secure workspaces, archive rooms, system rooms, and around the organization’s premises.
- In order to conduct supplier relations securely, policies are established for reviewing procurement services and managing changes; security requirements are determined in agreements made/to be made especially with IT suppliers where information security risks are expressed.

December 11, 2025

Uğur DALBELER

General Manager