Çolakoğlu Metalurji

INFORMATION SECURITY POLICY

Çolakoğlu® Metalurji A.Ş. is committed to taking any and all manner of necessary measures to achieve, administer, monitor, review, maintain, and improve information security. Çolakoğlu® Metalurji adheres to the following principles in any processes that fall within the scope of information security management:

- It gives importance to ensuring the security of operations associated with the products and services that it offers its customers and other stakeholders.
- It seeks to manage information security in ways that are integrated, compatible, and balanced with work and business processes. The security and continuity of information assets are essential to integrated, dynamic business strategies.
- It makes it a principle to take measures against any risks that might threaten the confidentiality, integrity, and/or accessibility of the products and services that it offers its customers and other stakeholders.
- It identifies information security objectives that are compatible with the aims of this policy and of the organization; at regular intervals it quantifies this compatibility and considers opportunities to make constant improvements.

Information security is possible only through the confidentiality, integrity, and accessibility of information assets.

- *Confidentiality* means that information assets must be accessible only to authorized persons.
- *Integrity* means that information assets must be complete and valid and must be protected against unauthorized changes.
- *Accessibility* means that information assets must be available to authorized persons immediately whenever they are needed.

While adhering strictly to the principles set out above, Çolakoğlu® Metalurji seeks to conduct its information security operations with the following aims:

- It plans, operates, and develops its information security management system (ISMS) in line with the internationally recognized ISO/IEC 27001:2013 Information Security Management System standard.
- It takes all necessary action to ensure that its ISMS is compliant with Turkey's Protection of Personal Data Act (Statute 6698) and with its associated laws, regulations, and administrative provisions. Management and teams to which management has assigned information security responsibilities take necessary measures needed to constantly improve the ISMS by identifying potential risks and opportunities and through internal audits, management reviews, and corrective action. All roles and responsibilities associated with information security are to be spelled out and assigned by management.
- Management provides resources for the conduct of activities that are essential to the operations of the ISMS.
- Any material or moral losses that might adversely affect the competitive positions of the company and/or its stakeholders are to be prevented.

Çolakoğlu Metalurji

- Management determines the scope of the ISMS by identifying information assets; when determining business strategies, management complies with applicable statutory and contractual obligations while also taking into consideration the information security expectations of customers, suppliers, business partners, and other interested parties.
- Information security risks are to be managed by assessing, analyzing, and dealing with them; measures are to be developed as necessary and efforts are to be made to prevent potential risks.
- No information, including the personal data of customers and other stakeholders, is to be allowed to fall into the hands of unauthorized persons.
- End-users are to be made aware of information security and such awareness is to be constantly increased.
- Information security is to be managed effectively so as to minimize any losses that might arise from lapses in it.
- Efforts are to be made as necessary to reduce the likelihood of information security lapses; when lapses do occur, they are to be responded to in a coordinated manner.
- Measures are to be taken to head off any interruptions in critical work/business processes; when interruptions do occur, the processes are to be restored to operational order within targeted recovery times.
- The confidentiality, integrity, and accessibility of any customer-owned information assets within the ISMS are to be maintained; the continuity of critical work/business processes involving customers is to be ensured.
- The ISMS is to be constantly improved.
- Measures are to be taken as necessary so as to ensure the security of the company's operational premises and their immediate vicinity, including but not limited to secure workspaces, archives, and system control rooms.
- For the secure conduct of dealings with suppliers, policies are to be developed that address the issues of reviewing procurement services and managing changes in such services. In any agreements that are entered into with information technology suppliers and in which information security risks are mentioned, specific attention is to be given to security requirements.

29 November 2018

Uğur DALBELER

General Manager