TAFALLA
IRON FOUNDRY

Information Security Policy

TAFALLA IRON FOUNDRY, S. COOP. is a cooperative specialized in the casting of iron parts, serving the automotive and industrial applications sectors. Its main activity focuses on the manufacturing of engine blocks and cylinder heads.

For this reason, the company has implemented an Information Security Management System (ISMS) with the objective of achieving customer satisfaction through established processes based on continuous improvement. This system ensures the continuity of information systems, minimizes risks, and guarantees the fulfillment of established objectives, thereby maintaining the confidentiality, integrity, and availability of information at all times.

To achieve this, we affirm our commitment to information security in accordance with the TISAX reference standards. Management establishes the following guiding principles:

- Leadership and competence: Management demonstrates commitment and leadership in developing and maintaining the Information Security Management System.
- Stakeholder engagement: Identify internal and external stakeholders involved in the ISMS and ensure compliance with their requirements.
- Organizational context: Understand the organization's context and determine the related opportunities and risks as a basis for planning actions to address, assume, or mitigate them.
- Customer satisfaction: Ensure customer satisfaction—including that of other interested parties in the company's results—in all activities and their potential social impact.
- Objectives and performance: Establish goals and objectives aimed at assessing performance in information security and promoting continuous improvement within the ISMS framework.
- Legal and contractual compliance: Fulfill all applicable legal requirements, commitments made with customers and stakeholders, and internal policies or procedures adopted by the company.
- Data protection: Guarantee the confidentiality, integrity, and availability of managed data and information systems—both in customer services and internal operations—preventing unauthorized alterations or misuse.
- Incident response: Ensure the ability to respond effectively to emergencies and restore critical services as quickly as possible.
- Risk management: Implement appropriate measures to address risks identified through asset evaluation and risk analysis.
- Training and awareness: Motivate and train all personnel to perform their duties correctly and in accordance with reference standards, providing a suitable environment for process development.
- Communication: Maintain open and effective communication both internally and with customers.
- Competence and motivation: Evaluate and ensure the technical competence of staff and promote their motivation to participate in continuous improvement initiatives.

- Supplier management: Monitor and maintain a continuous evaluation system for suppliers and subcontractors, especially those involved in ISMS-related activities.
- Infrastructure and equipment: Ensure that facilities and equipment are properly maintained and aligned with the company's activities, goals, and objectives.
- Process improvement: Continuously analyze all relevant processes and implement necessary improvements based on results and established objectives.

These principles are endorsed by Management, which provides the necessary means and resources for their implementation. They are made publicly available through this Information Security Policy, ensuring awareness and adherence at all levels of the organization.

Reviewed and approved by the Management Council in September 2025

Miguel Ugalde
Managing Director

M. Filomena Prieto
Finance and IT Manager