

Information security and protection of the information assets are an essential condition for achieving the business objectives of PCM DE GmbH.

The information security requirements are aligned with the organization's objectives and the Information Security Management System (ISMS) represents the tool that enables secure information sharing, correct execution of operations, and reduction of information-related risks to an acceptable level.

In this context, company activities must always be carried out ensuring appropriate levels of availability, integrity and confidentiality of information, through the adoption of a formal "Information Security Management System" (ISMS), consistent with the requirements expected by PCM DE GmbH stakeholders and in compliance with applicable regulations.

In particular, PCM DE GmbH has decided to apply the ISMS to:

protection of information concerning the process of producing automotive products, stored within the company and subject to exchange with external parties.

The general objectives of the ISMS, pursued with the commitment of the responsible person, are:

- demonstrate to internal and external stakeholders the company's ability to deliver IT services regularly while ensuring confidentiality and integrity of data
- minimize the risk of data loss and/or unavailability by planning and managing activities to guarantee service continuity
- carry out continuous and adequate risk analysis that constantly examines the vulnerabilities and threats associated with the activities covered by the system
- comply with applicable laws and regulations, contractual requirements, standards, and internal procedures
- promote cooperation, understanding and awareness of the ISMS among strategic suppliers
- conform to the principles and controls established by TISAX or other standards/regulations governing the company's business activities, in particular those relating to privacy and the security of personal data (GDPR)
- protect information, with particular attention to the correct retention and secure exchange of business information and data related thereto (TISAX).

All personnel, within the scope of their respective responsibilities, must report to the Information Security Management System Manager (RSGSI) any incidents detected and any weaknesses identified in the ISMS.

The entire organization is committed to supporting the implementation, operation and periodic review, as well as the continuous improvement, of the ISMS.

The company's senior management undertakes to pursue, with adequate means and resources, the objectives of this policy.