Information Security Policy

AT&S Austria Technologie & Systemtechnik Aktiengesellschaft

Contact: Chief Information Security Officer (CISO)
E-Mail: informationsecurity@ats.net
Metadata: Management Manual

History of modification

Version	Date	Description	Author
00	25.06.2021	D.GR.IT-ISMS-21E – Creation	M Chinnappa Bernard
01	09.11.2023	D.GR.IT-ISMS-21E – Renew and Update	M Chinnappa Bernard / Angadipuram Chandrasekaran
02	29.11.2023	Update	Stefan Heine
00	07.03.2024	New document numbering in case of ISO27001:2022 revision	Stefan Heine
01	09.05.2025	Update	Stefan Heine

Table of Contents

1 Introduction

This document describes the AT&S general information security policy. The purpose of this policy is to establish a framework for managing information security within AT&S. The regulations of this policy ensure the confidentiality, integrity and availability of information assets critical to our business and production processes.

2 Scope

This policy applies to all employees and authorized users of AT&S´s information assets.

3 Information Security Objectives

- Ensure the confidentiality, integrity, availability, accountability and auditability of AT&S information.
- Protect information assets against unauthorized access, disclosure, alteration, and destruction.
- Comply with applicable industry standards, relevant legal and contractual requirements.
- Continuously improve the information security management system (ISMS).

4 Information Security Strategy

Our information security strategy is designed to support AT&S overarching business objectives. Key risks are addressed through targeted measures, as illustrated in Figure 1. The guiding principles of this strategy define our core focus areas and initiatives, ensuring a balanced approach to strengthening our security posture while maintaining productivity and cost-efficiency. The implementation and adherence to recognized security standards, contractual and regulatory requirements are continuously evaluated through internal and external audits. These assessments, covering both technical and organizational dimensions, provide essential visibility into the maturity and effectiveness of our current information security capabilities.

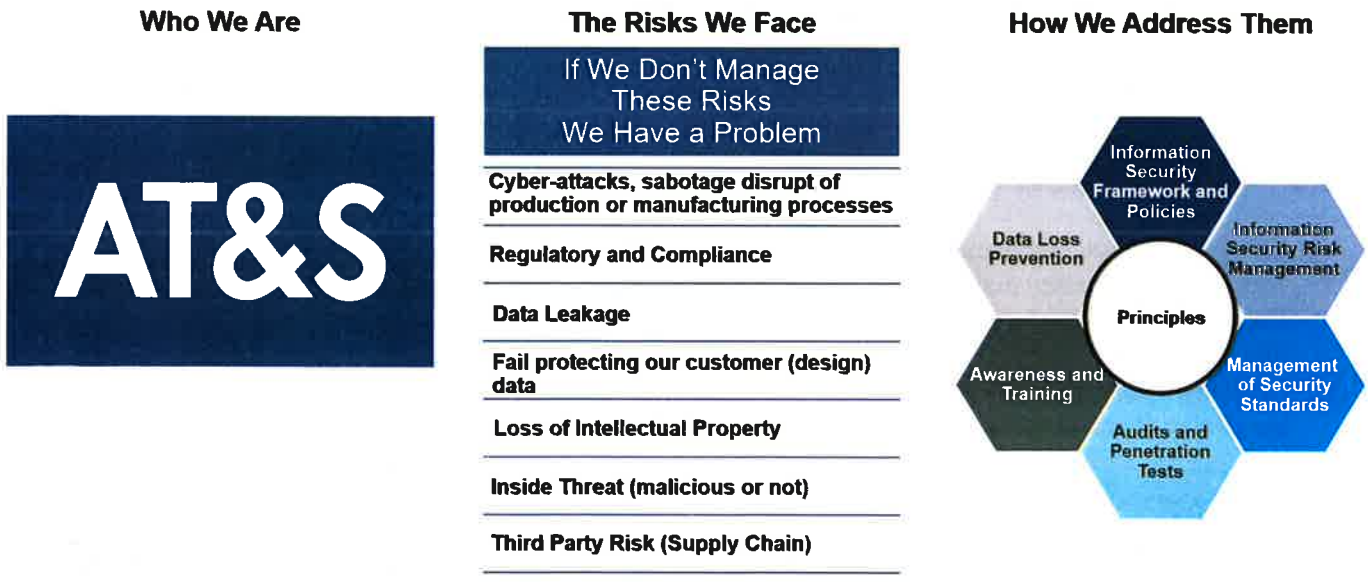

Figure 1

5 Essential Elements of the ISMS

- Carrying out a context analysis, considering the business activity and the requirements of interested parties
- Implementation of an appropriate information security awareness in all areas
- Establishment of operational organizational structures under the leadership of a CISO with sufficient competencies and the necessary financial and human resources
- Identify opportunities and risks of the ISMS and take appropriate measures
- Implementation of communication structures for information security
- Development and maintenance information security policies
- Measurement of the achievement of security objectives using KPI's
- Regularly audit the design and operational effectiveness of the ISMS
- Annual management evaluation and reporting of the effectiveness of the ISMS
- Definition and tracking of measures to eliminate non-conformities and the implementation of improvement measures by the responsible functional departments

6 Roles and Responsibilities

AT&S data, information and systems are overseen, utilized, and developed by various departments within the organization. The Information Security organization is responsible for establishing and maintaining a framework of policies and practices that must be implemented across all executive structures and enforced by accountable management.

The management board holds the ultimate responsibility for the established information management system. The management of AT&S has delegated authority for the implementation of this responsibility, with other key roles as described in following chapters:

6.1 Board of Management

- The management board is the top management of the group and overall accountable for the ISMS and committed to information security and continuous improvement.

6.2 Chief Information Security Officer

- Provide leadership and commitment to the ISMS, ensuring alignment with business objectives.

6.3 Information Security Manager

- Oversee the implementation and maintenance of the ISMS, including risk management and compliance.
- Responsible for policy maintenance, updates of those policies and their roll-out and acknowledgment.
- Reporting to the Chief Information Security Officer about relevant security incidents, improvements, audits and non-conformities.
- Local Information Security Managers are accountable for managing the ISMS at their respective sites, considering the unique characteristics of each location.
- Responsible for handling tasks, duties, projects, and other initiatives assigned by the CISO.

6.4 Business Process Owners / Functional Department Heads

- Ensure that information security controls are integrated to their area of responsibility and department processes.

6.5 Employees and Authorized Users

- Adhere to the relevant and applicable information security policies and procedures.

7 Compliance and Enforcement

- This policy ensures the organization's information security practices comply with ISMS standard ISO/IEC 27001:2022 and all applicable legal, regulatory, and contractual obligations. Ongoing compliance is verified through regular audits conducted as part of the ISMS.

- All employees and relevant stakeholders are responsible for adhering to the requirements outlined in this policy. You are obligated to review all detail regulations, documented in the complete set of Information Security policies, available in the AT&S document management system.

- Non-compliance with the company policies results in disciplinary action, up to and including termination of employment or contract.

8 Continuous Improvement

- Regularly review and update the information security policy to reflect changes in the production environment and emerging threats.
- Implement corrective actions to address nonconformities and improve the ISMS.

9 Communication

- Communicate this policy to all employees, contractors, and relevant third parties involved in production.
- Make the policy available to interested parties upon request.

10 Review and Approval

The information security policy will be reviewed annually by the Information Security Managers, CISO and approved by top management. Other ISMS policies will be reviewed annually and updated as necessary by the Information Security Managers and approved by the CISO and published within the organization.

11 Referenced Documents

All ISMS policies published in AT&S document management system.

Dr. Michael Mertin
Chief Executive Officer
Executive Board

Chief Finance Officer
Executive Board