Informations Security Management
Guideline Information Security

Table of Contents

1 Guiding Principle and Importance of Information Security

The ideas and expertise of our employees are the foundation of our success. The availability of our facilities, equipment, and systems, as well as our accessibility, reflects our reliability toward customers and business partners and significantly contributes to the good reputation of our company. To protect these values, our company establishes a worldwide, appropriate level of protection for the confidentiality, integrity (accuracy), and availability of our processes, information, and systems.
The declared corporate objective of effectively protecting core business processes along with the required information assets and IT systems is achieved through the creation of globally valid security standards and the integration of information security into internal processes. The defined information security objectives contribute to achieving the company's overall goals.
A constant awareness of information security in all daily activities is expected from every employee. Every supervisor is obligated to ensure and monitor compliance with information security regulations by their employees. Every employee who identifies weaknesses in the area of information security is required to report them to their supervisor or the Information Security Officer.

2 Our Expertise, Our Competitive Edge

Care and Accuracy in Handling Information

Need-to-Know Principle

Information should only be shared with individuals and entities that genuinely need it. The parties involved must clearly understand how confidential the information is and who it is intended for. This also applies to permissions in IT systems and access rights.

Proper Handling of Documents and Data Carriers

Handling documents and data carriers containing confidential content is a key aspect of protecting information. Minimizing the printing of sensitive information, securely storing documents and storage media in locked areas, and proper disposal are the responsibility of every employee.

Technical Security

The security level can be significantly strengthened through technical measures. Targeted investments in protection, as well as a secure design of our IT systems and buildings, are therefore also part of our security strategy. Our highest priority is to protect our most important and sensitive facilities.

Personal Responsibility

Every employee is responsible for reporting weaknesses, suspicious situations, and incidents. Knowing and complying with the established guidelines is considered a prerequisite and is expected from every employee

Implementation

The company uses an Information Security Management System (ISMS) based on the international standard ISO/IEC 27001 to ensure the implementation of information security requirements. In addition, legal and contractual requirements are taken into account.

The ISMS follows the recommended continuous improvement process based on the PDCA model (Plan, Do, Check, Act). The goal is to regularly and demonstrably ensure the appropriateness, completeness, sustainability, effectiveness, and efficiency of the implemented information security processes and protective measures.

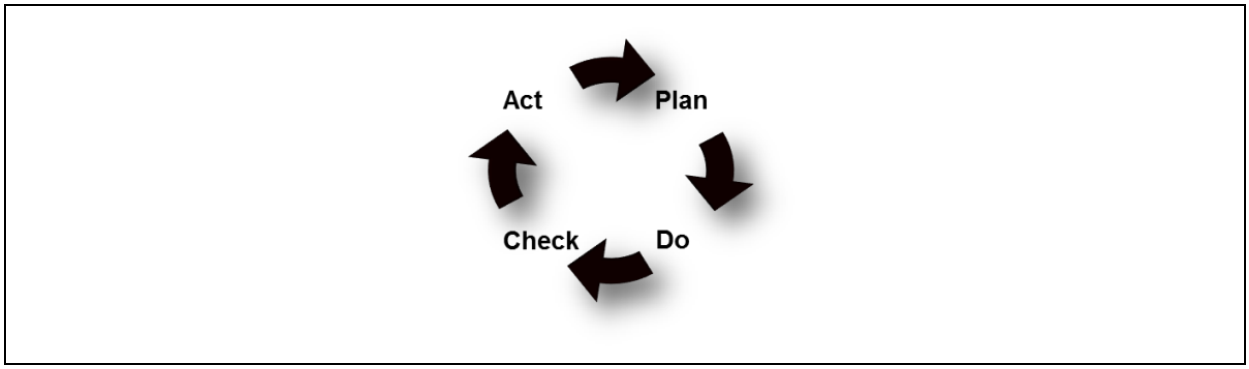

Abbildung 1: PDCA-Modell

PLAN - Establishing the ISMS: The strategies, objectives, processes, policies, procedures, methods, tools, and responsibilities of the ISMS are defined.

DO - Implementing and Executing the ISMS: The defined processes, policies, and procedures are implemented according to the ISMS objectives. Selected measures are put into practice.

CHECK - Monitoring and Reviewing the ISMS: Based on practical experience, audit results, and management reviews, the processes, effectiveness, and efficiency of the chosen approaches and measures are assessed and verified. It is identified whether action is needed and where optimization opportunities exist.

ACT - Maintaining and Improving the ISMS: Based on the results of the CHECK phase and other feedback (e.g., current risk situation, threat landscape, developments, requirements), corrective and preventive actions are taken to ensure continuous improvement of the ISMS and the security level. Handling security incidents is another task of this phase.

3 Overview Processes and Guidelines

Content
ISMS Prozess Risikomanagement
ISMS Prozess Zielemanagement
ISMS Prozess Auditmanagement
ISMS Prozess Umgang mit Informationssicherheitsvorfällen
ISMS Prozess IT-Notfallmanagement
ISMS Prozess Schulungsmanagement
ISMS Richtlinie Mitarbeiter
ISMS Richtlinie IT-Administratoren
ISMS Richtlinie Schutzklassenmanagement

4 Responsibility of Management

The company's management is responsible for information security within the organization and is committed to providing the necessary personnel, organizational, and financial resources to establish, maintain, and further develop an appropriate level of information security.

As part of their management duties and role model function, all executives are particularly responsible for promoting security awareness among their employees with regard to information security and IT security

5 Final Provisions and Scope of Application

This guideline is supplemented by additional directives consisting of detailed organizational and security rules in selected areas, as well as country- and site-specific legal and organizational regulations. Unless otherwise indicated, they have the same scope of application as this guideline and are valid from the date of their publication. The scope of the underlying Information Security Management System is centrally defined and described in detail in the applicable ISMS Scope document.