Information Security Policy

February 2024

Version 1/2024

Table of contents

Information Security Policy

Foreword by the Management Board

Responsible, sustainable management and profitable growth are guiding principles of our business activities.

We are convinced that a company must protect its values with the help of information security in order to be successful in the long term.

Cyber and information security threats are constantly increasing, and inadequate protection against these threats can have serious consequences for our business, our customers and our employees.

This policy defines the applicable Information Security Management System (“ISMS”) for KAP AG and its affiliated companies.

It applies to all executives and employees of the KAP Group and is a vital component of a successful future.

We ask all executives and employees of the KAP Group to carefully read this policy and adhere to it in their daily business.

KAP AG

Management Board

Marten Julius Dr. Hartmut Sauer

Basics

1. Information Security Goals

A key goal of information security is to reduce negative impact on KAP AG (“KAP”) and its affiliated companies (according to para. 290 sec. 1 HGB, “Affiliated Companies”) at home and abroad (together “KAP Group”) to an acceptable level of risk and is therefore part of the company-wide responsibility to manage business risk.

1.1 Protection of information assets

Information security is designed to protect information assets from the risk of loss, business interruption, misuse, unauthorized disclosure, inaccessibility and damage.

1.2 Protect customers, employees and reputation

Failure to protect information and services from cyber and information security threats can have serious consequences for our customers and employees.

Reputation, brand and financial stability can nevertheless be damaged.

The ISMS shall protect the trust of our customers, suppliers and other business partners, shareholders, employees and the general public in the integrity and reliability of the KAP Group and its products, thereby preserving and enhancing the reputation of the KAP Group and its Employees.

1.3 Compliance with legal obligations

The companies of the KAP Group operate worldwide. Numerous laws regulate cyber and information security as well as data protection across borders.

In some countries, there is a legal obligation to report data protection incidents / cyber-attacks in the event of a corresponding risk situation. The ISMS should also meet these requirements.

2. Scope of Application

This Information Security Policy ("Policy") sets out and governs the ISMS of the KAP Group.

This Policy applies to everybody employed by or temporarily working for the KAP Group as well as for external service providers performing group-internal tasks (each an “Employee”)

The ISMS serves to manage the legal and regulatory risks covered by the KAP Group's Code of Conduct and other policies supplementing it.

In particular, this Policy serves to:

- Determine the fundamentals of the ISMS and thus to provide orientation and
- support to Employees;
- Outline the structure and reporting lines within the KAP Group’s Information Security organization and define the interfaces with other functions; and

- Describe the process of and requirements for the active management of Information Security risks.

This Policy is supplemented by the Policies “Professional & Technical Requirements for Information Security” and “Information Security Requirements for Executives and Employees”, as well as the Data Protection Policy “Code of Conduct for Data Protection”.

Where there are stricter local laws and regulations than those set out in this Policy, these requirements must be complied with in the relevant jurisdiction.

2.1 Definitions

Information and Data: Information represents the content/meaning of data. Data is defined as the presentation of information in electronic form or other forms (e.g. stored on a hard disk, printed on paper, burned to a CD, copied to USB, conversations stored/archived as audio or video).

Information security: Defined as a method of protecting information and information systems from unauthorized access or misuse, disclosure, interruption and alteration, as well as from data loss or destruction. It is usually supported by organisational and technical measures.
Information Security is related to data protection and the goal of protecting the **Availability, Confidentiality, Integrity** and **Authenticity** of information.

Information value: An information value is information that is stored in any way and is valuable to KAP. The information could be customer, employee or company information that may be transmitted, processed or stored in any form inside or outside KAP's premises.
This includes, but is not limited to, oral, written, paper or electronic, as well as structured data in a database, application or any other form. Unstructured on a shared hard drive, SharePoint site, etc.

Data protection: Defined as the right of a data subject to decide and determine who is authorized to access their personal data, at what time and for what reason, and under what conditions their personal data may be used and disclosed to third parties.
Data protection deals with a subset of all the company's information and data. It relates exclusively to personal data, but in that context to information security too.

2.2 Principles of Information Security

Information security is based on the following principles:

Information Ownership - All information assets must be assigned to an owner who is responsible for its use within the organization. In this context, "accountability" means the responsibility to determine and maintain the security measures necessary to protect information assets. This is done through classification.

Classification of Information Assets - All information assets must be classified and treated according to their requirements for availability, confidentiality, integrity, and authenticity. Business

requirements as well as applicable legal, contractual or regulatory requirements and restrictions must be considered. In order to facilitate the implementation of continuous and effective information security measures, the basic model for the classification of information assets of KAP in accordance with the Guideline on the Classification and Handling of Information must be used.

Protection of information assets - Appropriate information security measures must consider business requirements, a risk assessment, economic efficiency, legal, contractual or regulatory requirements and restrictions and available technical and insurance safeguards. Since information and systems cannot be fully protected, the residual risks (the level of risk after the implementation of countermeasures) must be assessed, documented and processed.

Information Security Controls - A holistic approach is required when implementing information security controls. Such controls should not be considered or implemented in isolation. For example, whenever it is difficult to implement a particular measure, appropriate compensatory controls must be put in place.

System logging and monitoring - Methods must be in place to detect and log security breaches, anomalies, incidents, and unauthorized actions. Systems should be monitored and information security incidents recorded. User and error logs should be kept ensuring that system problems are detected.

Incident management and security breaches - Incident reporting processes are required to act reasonable and efficient, limiting or avoiding business disruptions and learning the lessons of incidents to minimize the risk of damage occurring in the future and improve safeguards. It is the responsibility of all Employees to report any breaches, weaknesses and disruptions.

Need-to-Know Principle - The Need-to-Know principle says that a user may only have access to the information that his or her job function requires. Access to information assets must be explicitly authorised. By default, there is no access.

Division of tasks / four-eyes principle - Valuable information and critical processes must never be controlled exclusively by one person. The sharing of tasks and the four-eyes principle should be applied in order to separate contrary skills or to identify integrity weaknesses or to prevent fraud in the handling of information.

Data Leakage Prevention (DLP) - Opportunities for data leaks must be limited. Data owners must determine the requirements for protection. Possible measures include restricting mass printing (email), downloading functions and copying to external media. Anonymize and mask data etc.

Access control measures - Access control measures are designed to prevent unauthorized persons from physically gaining access to equipment used to process or use information and personal data.

Access controls - Access control measures are designed to prevent systems from being used by unauthorised persons. Password management is required to implement this control measure, including two-factor authentication, password guidelines and appropriate logging of password usage for privileged accounts.

3. Information Security Strategy

This policy defines the framework for the management of information security. We strive for an appropriate level of security and align ourselves with international standards such as the

ISO27001, the European NIS2 Directive and the national IT-Grundschutz of the Federal Office for Information Security (BSI).

With the adoption of this Policy, the Management Board of KAP AG thus lays the foundation for the introduction of the ISMS. Supported by software, the ISMS defines standardized procedures, guidelines and predefined measures to protect corporate assets and minimize risks.

As a central authority, the Management Board of KAP AG appoints an Information Security Officer, who assumes responsibility for the topic of Information Security.

In his role, he reports to the management. In close cooperation with the Information Security organization, necessary measures are planned and implemented.

The Information Security Officer shall be provided with all necessary resources to perform his or her function. This includes suitable qualification opportunities in order to be able to react to current security-related issues.

In order to maintain and continuously improve Information Security, selected security measures are checked at regular intervals to ensure that those provide sufficient protection.

Reports of Security incident are analysed, documented and treated by the Information Security Organization. Appropriate reporting channels must be established.

It is essential that the company's employees report security risks and incidents.

4. Information Security Organization

The Management Board has overall responsibility for Information Security in the company. They can delegate Information Security management tasks to those responsible. Nevertheless, the overall responsibility always remains with the Management Board.

An information security organization is formed to plan, implement and maintain the security process. This consists of the following responsibilities:

- Information Security Officer
- Director IT / KAP AG
- IT Security Team
- Data Protection Officer
- IT-Management of the Subsidiaries / Representatives of the Segments

The organization must be supported in relevant areas by those responsible at management level. It must be regularly reviewed whether the organization that has been set up is still appropriate for its purpose or whether it needs to be adapted to new framework conditions.

4.1 Roles and Responsibilities

Information Security Officer ("ISO")

- Monitoring and evaluating the company's information security policies and procedures

- Identification of risks and threats to information security and development of measures to minimize these risks
- Training and awareness campaigns for employees on information security
- Security checks and audits in cooperation with internal and external auditors
- Security incident response and investigation
- Ensuring compliance with legal and regulatory requirements regarding information security

Director IT / KAP

- Responsible for the IT department of KAP
- Strategic management of the IT infrastructure of the entire Group in cooperation with the IT management of the subsidiaries / representatives of the segments
- Operational and strategic management of the IT infrastructure of the entire Group
- Planning and ensuring efficient, secure and reliable IT operations
- Developing and implementing an IT-strategy
- As Director IT of KAP, he is responsible for the planning, operation and further development of IT systems and processes within the organization

IT Security Team

- The IT Security Team is responsible for "Detection", "Response" and "Prevention" as well as other related activities
- The aim of the "Detection" task is to detect IT-security events promptly and reliable
- If necessary, the team will take appropriate action under the "Response" task area
- Findings on cyber risks, in particular threats, vulnerabilities and incidents, are recorded, analysed and processed in the "Prevention" area of responsibility

Data Protection Officer

- Checks whether the personal data in the company is sufficiently protected and whether the GDPR guidelines are implemented correctly
- If a data protection impact assessment has to be carried out, the Data Protection Officer advises the controller on this
- The Data Protection Officer is the interface between the company and the supervisory authority. He works with both sides and is the point of contact for specific questions
- Training and awareness campaigns for employees on the subject of data protection

IT Management of the Subsidiaries / Representatives of the Segments

- Responsible for the local IT department, IT applications and IT infrastructure
- Documenting and monitoring local IT assets
- The local IT management is responsible for all local IT risks
- Planning and ensuring efficient, secure and reliable local IT operations
- Local implementation of the group-wide IT- and Information Security strategy

However, responsibility for Information Security does not lie solely with the information security organization, the IT department, or the executives. **Every employee is responsible for the security of the organization's information and systems.**