Information Security Requirements for Employees and Line Managers

February 2024

Version 1/2024

Table of contents

Basics 1
1. Scope of Application 1
KAP AG Code of Conduct 1
2. Information Security Requirements for Employees 2
2.1 Passwords, credentials and access cards 2
2.2 Physical Security 2
2.3 Information Security 3
2.4 Secure communication 3
2.5 Protect your workplace and equipment 4
2.6 Social Engineering, Phishing & Malware 4
3. Line Manager Responsibilities 5

Basics

1. Scope of Application

This Information Security Requirements for Employees and Executives Policy ("Policy“) of KAP AG ("KAP") defines the requirements for Employees and Executives, as part of the Information Security Management System (the "ISMS") of KAP and its affiliated companies (according to para. 290 sec. 1 HGB, “Affiliated Companies”) at home and abroad (together “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 Directive is a supplement to the Information Security Directive and the Directive on Professional & Technical Requirements for Information Security, as well as the Data Protection Code (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.

Information relates to the content or meaning of data and can be stored in any way (physical copy, e-mail, file on the computer, etc.)

As defined in the Information Security Policy, Information Security is related to data protection and the goal of protecting the **Availability**, **Confidentiality**, **Integrity** and **Authenticity** of information.

Cybersecurity is the process of protecting information against digital threats. Cyber and information security measures span the entire life cycle of information.

KAP Code of Conduct

Protection of confidential information

The KAP Group ensures that sensitive data (business secrets and personal data) is collected, processed, secured and deleted appropriately and in accordance with the law. It obligates its employees accordingly. Data worthy of protection may not be passed on to third parties without authorization or published in any other form and must be protected accordingly.

The KAP Group protects company data as well as personal customer and employee data against unauthorized access, unauthorized or improper use, loss and premature destruction using all suitable and appropriate technical and organizational means available to the Group.

All employees are therefore obliged to take the necessary measures to ensure the security of IT systems with regard to internal and external misuse and threats. In addition, the company ensures the utmost care and strict confidentiality when collecting, storing, processing and transferring personal data of employees, customers or other third parties, as well as compliance with applicable laws and regulations.

2. Information Security Requirements for Employees

To protect our customers, partners and colleagues, we are required to protect information from cyber and information security risks.

This document is intended to clarify why it is important for everyone to protect information. It defines the requirements for employees and executives and provides advice on how to apply them in their daily work.

2.1 Passwords, credentials and access cards

Your login credentials, including passwords, PINs, tokens and access cards, are personal data that may only be used by you. Never share your credentials, as they only allow you access to systems and facilities and are equivalent to your personal signature.

You are responsible for any action taken with your credentials. Therefore, the following rules apply for your credentials including passwords, PINs, tokens or access cards:

- May not be passed on to anyone, regardless of rank or role
- Must be protected against theft or misuse and immediately report the loss or potential misuse to your manager and the Information Security Organization
- May only be used for authorized purposes

2.2 Physical Security

Information Security goes beyond digital and includes the protection of information in physical form.

You are responsible for your access card/chip and may never pass it on to others.
Access through controlled doors and barriers may only be granted to authorised persons.

Your visitors must register and may only be admitted to a building or area if accompanied and supervised. Any suspicious person or activity must be immediately reported to those responsible for physical security.

To secure physical documents, you must follow the "Clear Desk" rules for a secure workplace. This applies to your own workspace in the office, home office and in shared areas.
The following Clear Desk rules apply:

- Lock your screen with a (password-) protected screensaver, even if you only leave the workplace for a short time
- Never leave "confidential" or "strictly confidential" documents unattended at your workplace or in the printer
- Close windows and doors when no one are in the office
- Carry mobile devices with you or lock them away
- Dispose data and information safely, e.g. a USB stick with company data in a secure data disposal container, internal documents in the shredder
- When using meeting rooms as well as central copiers, printers and fax machines, be aware of the security rules and don’t let internal documents lying around unattended

2.3 Information Security

Information refers to the content or meaning of data and can be kept in any form, e.g., email, file on desktop, physical copy, etc.

As defined in the Information Security Policy, information security is the protection of the confidentiality, integrity, availability, and authenticity of information.

Information, regardless of its form, must be protected based on the classification assigned. This applies throughout the entire life cycle

The information lifecycle includes:

a) Building
b) Handling and transport
c) Storage and archiving
d) Destruction and disposal

You, as the owner of the information, are responsible for ensuring that the information you create is classified according to its confidentiality. This is governed by the Classification & Handling of Information Guideline.

- If you create new information or make significant changes to existing information, you will need to re-visit the confidentiality classification
- Information is always subject to the level of protection required by the owner of the information
- The default classification for information is "internal"
- Information that is classified as "confidential" or above must be labeled with the appropriate classification

2.4 Secure communication

The Internet, e-mails, messaging services and virtual conferences are more and more essential tools in our daily professional and private life.

Unfortunately, these also represent the risk to expose for Cyberattacks and shouldn’t be underestimated. Small mistakes or lack of attention to detail can have major consequences.

You must only use authorized communication channels and systems provided by the company for your business communication.

You must ensure that the distribution of information through authorized channels is appropriate and is always reviewed and acted upon on a "need to know" basis.

The "need to know" principle is the requirement to limit access rights to information and systems to what is necessary for a person to perform his or her duties.

- When distributing information that is not classified as "public", efforts must be made to ensure that all recipients and participants are authenticated before sharing/distribution begins.
- Information that is protected on a shared storage system with access controls may only be disclosed to authorized persons ("Need to Know")
- Only authorized online storage systems / file share services must be used

- External storage media / removable storage devices may only be used in exceptional cases, including USB sticks, external hard drives, CDs, DVDs. These must be checked for viruses or other malware before used.
- Information distributed with such media must be encrypted and potential losses must be reported.
- Voice controlled smart devices make it possible to be activated using voice recognition. This can be very convenient, but in order to keep your business conversations safe at home, it is recommended to disable these services.
- Use your business email address exclusively for business purposes and do not provide any details about the company, your role, your colleagues or similar in social media channels.

2.5 Protect your workplace and equipment

Electronic devices are used every day and they are the primary means with which we access information and perform our roles. In addition, the internet continues to be an indispensable business tool. However, both electronic devices and the internet are key routes that may be used to attack us.

Proper use of the devices and software provided is essential for the protection of information.

- You must only use approved hardware, software and services software provided by the company to access, process or store company data
- You must not by-pass, modify or undermine any technical or organizational security controls
- Unusual changes to the equipment of your workplace, such as replaced systems, additional hardware, manipulated software or missing peripheral devices, must be questioned and reported
- You must report lost or stolen devices immediately
- When you leave the company, you must return all electronic devices

2.6 Social Engineering, Phishing & Malware

As an employee, you may be targeted by malicious individuals to gain access to the company's information and systems.

Social engineering is the act of developing trust with individuals for malicious purposes. In this way, criminals tempt the victim, for example, to disclose information, bypass security controls, make bank transfers or install malware on a private device or a computer on the company network.

Phishing is a type of social engineering in which fraudulent emails, instant messages, voice (bogus calls) and websites are used to deceive individuals into clicking links or opening attachments in order to install malware on systems or to obtain sensitive information like login credentials.

You should be aware of the risks posed by cyber threats, malware, and social engineering, and take steps to mitigate these risks.

- You should be aware of the risks posed by cyber threats, malware, and social engineering, and take steps to mitigate these risks
- It is essential to work through and understand the training materials and guidelines provided on the subject of information security and cybersecurity in a timely manner

- Never allow an unauthorized person to remotely access or control your device. If you do so, report it to the IT department immediately
- Report unusual activity on your electronic devices, as well as suspicious requests for information from strangers, which you deny
- Phishing e-mails can be forwarded in Outlook, for example, via a "Report spam to IT" button.

3. Line Manager Responsibilities

Line Managers have additional Information Security responsibilities towards their employees and the company as part of their supervisory and duty of care.

You have to pass on important messages from this area to your employees and you are the recipient of their reports about anomalies and activities that could affect Information Security.

In addition, they also review the access rights of their employees to information and systems, this is especially important in regard to joiner, mover and leavers. They are responsible for the implementation and control of the "Need to Know" principle in their area.

However, the most important aspect of their additional responsibilities is the obligation to foster an appropriate and proactive Information Security culture among their employees.

The Information Security culture is a component of the corporate culture and determines the perception, thinking, feeling and acting in relation to Information Security.

- Check the access rights and permissions of your employees regularly
- When approving new access rights and permissions, always act according to the "need to know" and "least privilege" principle
- They must ensure that the HR department is informed in time so that changes and departures affecting their employees can be implemented promptly
- They must ensure the return of their employees' electronic devices and access cards when they leave the company