Professional &Technical Requirements for Information Security

February 2024

Version 1/2024

Table of contents

Basics

1. Scope of Application

This ("**Policy**") of KAP AG ("KAP") regulates functional and technical requirements for information security, as a component of the Information Security Management System **("ISMS**") of KAP and its subsidiaries (within the meaning of Section 290 (1) of the German Commercial Code (HGB), **"Subsidiaries**") in Germany and abroad (collectively "**KAP Group**").

It applies mainly to departments that can implement technical and organizational measures. This includes IT responsible managers and employees, human resources, facility management and temporary IT employees of the KAP Group, as well as external service providers who are employed within the Group in these Areas ("**Employees**").

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 stricter local laws and regulations apply 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 Directive, information security is the protection of the confidentiality, integrity, availability, and authenticity of information in any form.

Cybersecurity is the process of protecting information against digital threats. Cyber and information security measures extend over the entire lifecycle of information.

This Policy applies to all (IT) systems, regardless of whether they are developed in-house or purchased externally.

2. Information Management Requirements

Information owners have a responsibility to ensure that the information they create is classified according to its sensitivity.

All information, regardless of its form, must be protected based on the classification assigned to them.

Information protection and management focuses on determining the level of protection of information assets and the resulting requirements.

Measures must be defined to maintain this level of protection throughout the entire lifecycle. This includes protection in transit, at rest, and the application of appropriate access controls.

2.1 Protect information throughout its lifecycle

2.1.1 Requirements must be defined to enable the information owner to properly classify their information in terms of confidentiality

2.1.2 These requirements must also consider the risk of data loss or data theft that can impact the integrity of the data

2.1.3 Requirements must be defined by the business to ensure the availability of information accordingly. This has an impact on backup and capacity management systems

2.1.4 IT Security and the ISO define the technical requirements to protect against data leakage based on information classification

2.1.5 Company owned data must only be available on authorized hardware and software

2.1.6 Access to data must be restricted to identified, authorized, and legitimate individuals

2.1.7 Information must be protected by encryption during transport, according to its classification:

- In public areas and networks, if internal or higher classified
- Whenever classified as strictly confidential

2.1.8 To prevent data loss from lost and stolen devices, mobile devices must be protected with encryption

2.1.9 Information or IT systems that are no longer needed must be deleted or destroyed following a "secure" procedure

2.2 Control information distribution

2.2.1 IT Security, in cooperation with the Information Security Officer, must develop strategies and implement a system to monitor and control outgoing communications to protect against unwanted data leakage

2.2.2 External communication channels must be monitored to prevent data loss and the spread of inappropriate content

2.2.3 Unauthorized communication channels must be identified and blocked.

2.2.4 Where external communication channels of applications are not disabled, measures must be taken to protect against data loss.

2.2.5 Access must be blocked to websites with inappropriate or illegal content

2.2.6 Based on the classification of information, the requirements and risk appetite for data loss protection must be defined

2.2.7 Risks and exceptions must be managed within an acceptable level. The assessment of cyber and information security risks and the effectiveness of countermeasures must be consistent with the strategy of the risk framework and risk appetite

3. IT-Asset Management

Every informational transaction relies on the security of our infrastructure. IT asset management is the set of practices that ensure that IT assets are properly managed throughout their lifecycles.

The asset inventory must be regularly reviewed and updated. As part of changes to the IT infrastructure, updating the IT Asset Register must be an integral part of the planning and implementation work.

IT asset managers are required to capture IT assets and document the following information:

a) Relevant cyber and information security parameters, based on classification according to the confidentiality, integrity, and availability of the asset
b) For effective technical vulnerability management, the inventory must include the software vendor, software name, version numbers, and current state of deployment
c) The process-related dependencies between applications, software packages, and the infrastructure they require to operate

3.1 Standardized and consistent inventory

3.1.1 The inventory includes all hardware and software data available in the organization, whether physical, virtual, mobile or in the cloud

3.1.2 The inventory must be carried out consistent, standardized using suitable tools

3.2 Responsibilities and Assignment

3.2.1 Each IT asset must have a defined IT asset owner who is accountable for the asset. Ownership of IT assets needs to be documented, managed, and updated, especially when owners change or leave the organization.

3.2.2 IT managers nominate an IT asset manager for their area of responsibility.

3.2.3 Central IT management must define and manage a data quality process

3.3 Protection against unauthorized access, modification or damage

3.3.1 Systems and infrastructures must be protected against unauthorized access, damage or modification

3.3.2 Unauthorized IT/IoT devices must be detected and isolated by a network procedure

3.3.3 Detected, unauthorized devices must be approved or removed as soon as possible

3.4 Rules for the secure use of information and IT assets

3.4.1 Mobile devices used for the company, such as smartphones, tablets and laptops, must be managed with a management system. Management includes updating software and device settings, monitoring compliance with organizational policies, and remotely wiping or locking devices

3.4.2 Software or other components may not be downloaded, installed, deployed, or used unless licensed to the Company

3.4.3 By default, all protocols and services that are not explicitly approved for use over the Internet must be blocked

3.4.4 There must be a process in place to adequately control and manage internet usage and other external connections

3.4.5 Firewalls must be established between the Internet and the internal networks, this also applies to cloud environments

3.5 Ensuring safe and resilient operation

3.5.1 The configuration settings that are relevant to maintain the confidentiality, integrity, and availability of infrastructure components must be defined, tested and approved, before they are deployed to production

3.5.2 Configuration settings must be regularly reviewed and updated to reflect changes in underlying security requirements

3.5.3 Changes to firewall rules must be approved and subject to a defined change management process. Regularly, at least once a year, these rules must be validated and if necessary, updated or removed

3.5.4 Where security certificates are used, it is important to ensure that a process is in place to monitor and renew those

3.5.5 The lifecycle of applications and infrastructure components must be managed to identify those that are nearing end-of-life, to deploy security patches or hotfixes

3.5.6 For end-of-life solutions that are no longer supported by the relevant provider, additional controls must be put in place to maintain an acceptable level of risk

3.5.7 Information on technical vulnerabilities of systems used should be obtained in a timely manner, the exposure to such vulnerabilities to the organization should be assessed, and appropriate measures be taken to address the associated risk. This includes:

a) Define and establish tasks and responsibilities that include vulnerability monitoring and risk assessment, patching, asset tracking and any necessary coordination tasks
b) A timeline to respond to relevant technical vulnerabilities. Critical systems should be prioritized
c) Patches should be tested and evaluated prior to installation to avoid issues
d) If a patch is not available, other measures should be considered:
    i. Shutdown of the services/functions affected by the vulnerability
    ii. Modify access controls, e.g. firewalls, network boundaries
    iii. Increased monitoring to detect attacks that are taking place
    iv. Sensitization of employees to the vulnerability
    v. All actions carried out should be documented

3.5.8 Detection, prevention, and recovery measures to protect against malware must be implemented and include, but are not limited to:

a) Install and regularly update malware detection and repair software for routine scanning of computers and other media
b) Scanning all files received over networks or obtained via a storage medium for malware, before use
c) Scan email attachments and downloaded files for malware, before use

3.6 Network Security

3.6.1 Network connection activity must be monitored and controlled to identify and escalate security incidents based on defined threat use cases

3.6.2 Network connections may only be allowed for approved and authenticated segments, people, and devices in accordance with access management requirements

3.6.3 Network connections that go through public networks must be encrypted

3.6.4 Documentation of sensitive network settings must be stored, kept up-to-date, and available on a least-privilege basis

3.6.5 Network diagrams are highly confidential and must be maintained to allow for faster recovery of systems in the event of security incidents

3.6.6 Users should only have access to those networks and network services that they are authorized to use

3.7 Data Backup & Recovery

3.7.1 Systems, applications and data must be backed up according to documented backup and recovery requirements

3.7.2 A policy should be created that specifies basic backup and recovery requirements, as well as retention and protection requirements

3.7.3 Adequate data backup systems and facilities should be in place to ensure that all critical data and applications can be recovered after an incident or media outage

3.7.4 When establishing a data backup plan, the following points should be considered:

a) Accurate and complete records of backup copies and documented recovery procedures should be maintained
b) An overview should be kept that lists the location and content of the backups
c) The scope (e.g., full or incremental backup) and frequency of backups should reflect the organization's business needs, the security requirements of the information in question and the importance of the information to business continuity
d) the backups should be kept in an off-site location at a sufficient distance to be protected from damage to the main site
e) the backups should have adequate protection against physical and environmental factors in accordance with the standards applied at the main site
f) Backups should be checked regularly to ensure that they can be relied upon in the event of an emergency. This should be done along with a review of recovery procedures coupled with a review of the time it takes to recover
g) As part of the operating procedures, the performance of data backups should be monitored and measures defined in the event of failed data backups to ensure the completeness of the backups
h) Where confidentiality is particularly important, data backups should be protected by means of encryption

4. Identity & Access Management

Access to resources requiring protection must be restricted to authorized users and authorized IT components. Users and IT components must be clearly identified and authenticated. Access Management is the control of access to our information, systems, services and premises.

4.1 Access Rights / Logical Access

4.1.1 There needs to be a process in place to effectively manage and assign permissions to joiners, movers and leavers, including:

a) Immediately disable access or delete the identifiers of users who have left the organization
b) Periodic identification and deletion or deactivation of redundant user IDs
c) Ensuring that previously used identifiers are not assigned to other users,
d) The process must allow for notifications and an approval process

4.1.2 User rights are assigned and managed in accordance with existing authorization concepts and guidelines

4.1.3 User accounts may only be associated with one person and it is generally not permitted to share user accounts with other people

4.1.4 Authorisations should be limited to the minimum requirements, i.e. according to the principle of least privilege

4.1.5 Permissions may only be deployed if they have been properly approved and comply with the defined approval workflow

4.1.6 Privileged access may be activated and used for valid use cases only

4.1.7 Activity of accounts with privileged access to the production environment must be logged to support auditability and security monitoring

4.1.8 The default setting is no access to local administrator rights for workstations. Exceptions may only be granted for temporary, administrative access that is supported by a valid use case

4.1.9 For IT staff, the following use cases are approved:

a) Integration of third-party software
b) Support tasks that can't be performed with standard tools
c) Software Evaluation and System Installation

4.1.10 Non-personal, technical accounts must:

a) Be registered in a repository and be associated with an owner
b) They must be securely configured to prevent unauthorized use, i.e. comply with the requirement for secure passwords, with the prohibition of disclosure and restricted allocation to authorized personnel only

4.1.11 Built-in default accounts of third-party products must be disabled, where this is not possible, the initial password must be changed immediately

4.1.12 A process needs to be defined that establishes use cases and the level of approval required to access someone else's data (active or former). This process is carried out in coordination with the HR department and the legal and compliance department with regard to the legal requirements. The IT department needs to implement this process to ensure that the required data can be made available.

4.2 Authentication

4.2.1 An appropriate authentication method must be chosen to confirm the user's identity

4.2.2 For strong authentication and identity verification (multi-factor), authentication alternatives to passwords such as cryptographic methods, smart cards or tokens must be used

4.3 Secure Login Procedures

4.3.1 A good, secure login procedure should:

a) Do not display system or application identifiers until the login process has been successfully completed
b) Display a general warning message that only authorized users should have access to the system
c) Do not display help texts during the registration process that could be used by unauthorized persons
d) the login data will only be checked after all data has been entered
e) When an error occurs, the system should not show which part of the entered data was correct/incorrect
f) protect against brute force login attempts
g) log unsuccessful and successful login attempts
h) trigger a security event when an attempt or successful credential bypass is detected
a) Do not display the password which was entered
b) Don't transmit passwords over the network in plain text
c) Terminate inactive sessions after a predetermined period of time, especially in locations such as public or external areas that are not under the organization's security management

d) Limit connection times for applications with high risk to provide additional security and minimize the opportunity for unauthorized access attempts

4.3.2 After successful login, you should see the following data:
e) Date and time of last successful login
f) Details of unsuccessful login attempts since the last successful login

4.3.3 The use of tools that may be able to circumvent system and application protection measures must be restricted and strictly monitored

5. Physical and environmental security

Unauthorized access, damage and interference with information and information processing facilities of the organization must be prevented. Loss, damage, theft or endangerment of assets and the interruption of organizational activities must be prevented. Security areas must be identified and documented accordingly.

5.1 Physical Security Perimeters

5.1.1 In a building or site where information processing facilities are located, security requirements apply, which should depend on the information values and the results of a risk assessment

5.1.2 Physical access to buildings or sites must be secured and controlled, and access must only be granted to authorised persons

5.1.3 Information processing facilities under the organization's control should be physically separate from those managed by external parties

5.1.4 Suitable burglar alarm systems, that comply with common standard should be installed and checked regularly

5.1.5 Fire doors in secure areas should have alarms and be monitored and checked

5.2 Physical access control

5.2.1 Security areas should be protected by appropriate access control to ensure that only authorised persons have access.

5.2.2 Check-in and check-out of visitors should be noted with the date and time, and all visitors should be supervised unless their stay has been pre-approved.

5.2.3 Visitors should only be allowed to enter for specific, authorised purposes and should be briefed on the safety requirements and emergency procedures in that area.

5.2.4 The identity of visitors should be confirmed in an appropriate manner

5.2.5 Access to areas where confidential information is processed or stored should be restricted to authorised persons by means of appropriate access controls, such as two-factor authentication mechanism e.g. an access card and a secret PIN

5.2.6 There should be a physical or electronic log, which is securely stored and monitored

5.2.7 All employees, contractors and external parties should be required to wear visible identification signs on the sites or buildings

5.2.8 Employees of third-party service providers should only be granted necessarily access to secure restricted areas or facilities, where confidential information is processed. This access should be specifically authorised and monitored;

5.2.9 Access rights to secure, restricted areas should be regularly reviewed updated and, if necessary, revoked

5.3 Working in secure areas

5.3.1 Employees should only be informed about the existence of secure areas or secure activities, when necessary

5.3.2 For security reasons and to prevent malicious acts, unsupervised activities in secure restricted areas should be avoided

5.3.3 Unused secure areas should be locked and checked regularly

5.3.4 The carrying of cameras and other recording devices, such as mobile phones, should be prohibited and only permitted with explicit permission.

5.4 Delivery and loading areas

5.4.1 Delivery and loading areas or other entrance points, where unauthorised persons could enter the premises, should be monitored and, if possible, separated from information processing facilities, in order to prevent unauthorised access

5.4.2 Deliveries should be registered at the site and inspected for tampering. If there are any signs of tampering, they should be reported immediately to security

6. Personnel security

All persons applying for a job should be subject to a security check. This screening must be in accordance with relevant laws, regulations and ethical principles. An appropriate relation to the business requirements, the classification of the information to be obtained and the perceived risks is necessary.

6.1 Vetting

6.1.1 Security checks should consider all data protection, privacy and employee related legislation and, where permitted, include:

a) Satisfactory certificates of good conduct, e.g. an official job reference
b) A CV of the applicant checked for completeness and accuracy
c) Confirmation of stated academic and professional qualifications
d) Independent identity verification (passport or similar document)

6.1.2 If a person is hired for a specific information security role, organizations should ensure that the applicant:

a) Has the necessary competence for the role
b) Has the required trustworthiness, especially if the role is critical to the organization

6.2 Terms and Conditions of Employment and Contract

Contractual agreements with employees and contractors should define their responsibilities and those of the organization.

6.3 Education and training in information security

All employees of the organization should receive appropriate awareness through education and training and regular updates on the organization's policies and procedures relevant to their professional field of work.

6.3.1 An information security awareness programme should aim to make employees aware of their responsibilities for information security.

6.3.2 Education and training on information security should take place on a regular basis. Initial training applies not only to new joiners, but also to employees who have been transferred to other positions or functions with significantly different information security requirements.

6.3.3 Education and training in information security should include general aspects such as:

a) Outlining management's commitment to information security in the organization
b) The need to become familiar with and comply with applicable information security rules and obligations

c) Personal responsibility for own actions and omissions, as well as responsibilities to protect information belonging to the organization
d) Basic information security procedures (such as reporting information security incidents) and basic security measures (such as password security, malware measures and clear desk)
e) Point of contacts and resources for further information, recommendations and questions, including further information security education and training materials

6.4 Violation process

6.4.1 A friendly and transparent violation process should be in place to take measures when an information security breach has occurred

6.4.2 A violation process should not be initiated without first checking if an information security breach has actually occurred

6.4.3 A formal violation process should ensure correct and fair treatment

6.5 Termination and change of employment

6.5.1 Responsibilities and obligations in the area of information security, which remain in place even after termination or change of employment, should be defined, communicated to the employee and enforced

6.5.2 The responsibilities and obligations that continue to apply after the termination of the employment should be described in the terms and conditions of employment

6.5.3 Changes in responsibilities or employment should be regulated in the same way as the termination of current responsibilities or employment

7. Use of passwords

Since passwords can be compromised and decrypted, certain rules and requirements must comply with to ensure a secure password. The following password rules have been developed with security requirements in mind and offer a high level of security when used consistently

7.1 Password rules

7.1.1 Every user is obliged to treat passwords provided to him or used by him confidentially and to keep them secret so that they are not accessible to third parties. Passwords must not be shared with third parties, colleagues or IT administrators

7.1.2 Passwords must not be stored in files or scripts, nor stored at the workplace, e.g. on pieces of paper, or programmed to function keys

7.1.3 Logon must never be made under someone else username/password

7.1.4 If there is any suspicion of loss of confidentiality or compromise, the password must be changed immediately. Otherwise, passwords must be changed at intervals of 180 days. A password that differs from the passwords used so far must be chosen

7.1.5 Preset passwords (e.g. of the manufacturer or IT admins for installation of systems) may only be used once and must be replaced immediately by individual passwords

7.1.6 Passwords that have already been used may not be reused after a password change

7.1.7 Passwords must be entered hidden to prevent unauthorised access

7.1.8 If misuse is suspected, the IT department must be contacted immediately

7.1.9 The password must be at least 8 characters long. It must consist of uppercase and lowercase letters and at least one digit and one special character (e.g., *'§$%& etc.) and must contain no more than two consecutive identical characters

7.1.10 No trivial passwords may be used, this includes consecutive letters and numbers, e.g., 123456 or abcdefg, or consecutive keyboard characters, e.g., asdfgh

7.1.11 It is also not allowed to use passwords that can be associated with the individual employee, e.g. name, place of residence, license plate number, etc., and no names/terms that can be found in dictionaries

7.1.12 The user ID must not be part of the password

7.1.13 The "Remember Password" feature offered by some browsers may not be used

7.1.14 Passwords that are used within the company may not be used in the same way in other environments (e.g. on the Internet, on customer portals, etc.).

7.1.15 In order to keep the risks as low as possible in the event of a password compromise, the same password should not be used for several systems or applications within the company

7.1.16 After several incorrect entries (three to five failed attempts), access must be blocked and may only be released again after the user has been identified beyond doubt

Compliance with these password rules must be automatically controlled and enforced to a sufficient extent.

8. Information security in relationships with third parties

While we use third parties such as suppliers, service providers, consultants or distributors to support and provide services for business functions across the company, we cannot delegate our responsibility for protecting information. Cyber and information security requirements related to third-party activities and supply chains are essential to meet our commitment to protect our information in all its forms. This applies in particular if the third-party stores or transmits data or if we have established a network connection with the third-party

8.1 Third Party Cyber and Information Security Requirements

8.1.1 Measures on cyber and information security requirements must be defined and requested to specifically govern third-party access to the organization's information. These include:

a) An assessment of cyber and information security controls must be part of the third-party selection process initiated by the business function that wishes to engage a third party

b) Minimum information security requirements for each type of information and access as the basis for each contract, according to business needs, requirements and risk profile

c) Identify and document the types of third-party service providers, e.g. IT services, logistics and utilities

d) A standardized process and lifecycle to manage the third-party relationship

e) Determining of the respective manner in which information is accessed, as well as monitoring and controlling access

f) Accuracy and completeness check to ensure the integrity of the information and/or the information processing carried out by each party

g) Regular reviews of the agreed controls must be carried out, based on repeatable and measurable evaluation mechanism

h) Arrangements for dealing with incidents and threats related to supplier access, including responsibilities on both sides

i) Arrangements for resiliency, recovery, and disaster where appropriate, to ensure the availability of information or information processing carried out by each party

j) Management of the necessary transfer of information, information processing facilities, etc. and ensuring that information security is maintained throughout the whole transfer phase

k) For planned and unplanned terminations of contractual relationships, regulations must be made that determine how all information, data and hardware of the users are to be returned by third parties (termination concept)

8.2 Third Party Risk Management

8.2.1 Prior to entering into a contract with a third party that provides services or products to us, a risk assessment of the third party's cyber and information security controls must be carried out that is adequate with the risk posed by the use of the third party

8.2.2 By means of an analysis based on an assessment of possible risks and their classification, it must be clarified whether the activity or process to be outsourced is to be assessed from a risk point of view with a high risk for the institution and if further measures may have to be taken