User Responsibility for Information Security Policy

1. Introduction The business processes of the COMPANY are geared towards mass processing. They must meet high standards of efficiency and quality, which is only possible through the use of IT, such as for automating processes or supporting administrative tasks. The use of IT in almost all areas of activity places particularly high demands on information processing security. The COMPANY meets these demands with a variety of technical measures.

However, the behavior of employees is also crucial for protecting information. Only if employees are aware of their responsibility for information security and actively support security measures can information be effectively protected. This document contains the essential regulations that all employees must know and apply to contribute to information security at the COMPANY. By doing so, they contribute to the company's long-term success. Additional specific regulations are described in further policies.

2. Notes In the following document, the terms "appropriate" and "fundamental" are used.

- The term "appropriate" is used when employees have discretion in choosing measures. The decision for specific measures must be made in accordance with the respective supervisor, considering the cost-benefit aspect.
- The term "fundamental" is used when employees can deviate from the regulation with justifiable reasons in exceptional cases. The decision against the regulation must be made in accordance with the respective supervisor, considering the cost-benefit aspect.

3. Areas of Responsibility

3.1 Data and Information Internal confidential data of the COMPANY may not be disclosed to external persons without prior approval from the direct supervisor. Such data may also not be transferred to IT devices and networks not under the sole control of the COMPANY. In particular, the transfer of these data to private IT devices and networks of the COMPANY's employees is prohibited to perform work assignments in the home environment.

Employees of the COMPANY are obliged to classify information according to its protection needs and, if possible, to label it accordingly. Classified information must be handled according to its protection class.

3.2 Workplace The following regulations apply to all workplaces of the COMPANY:

- The principle of a "clean desk" (Clear Desk Policy) applies. This means that all data carriers, especially documents with confidential content, must be locked away when leaving the workplace.
- Documents such as work instructions, presentations, and diagrams must be classified and handled according to the rules for the respective classification.

- For printing confidential documents or personal data, the Follow-me printer or a PIN1 must be used unless the printer is directly at the workplace. If neither is possible, printouts must be collected from the printer immediately. Supervisors are obliged to ensure through appropriate organizational measures that uncollected printouts to which unauthorized persons could have access are regularly removed from the printers at reasonable intervals.
- Documents with confidential content or personal data that are no longer needed in paper form must be disposed of in marked, locked containers or provided shredders.
- Office spaces must be locked when leaving, if possible and necessary.

3.3 Workplace Devices The COMPANY provides its employees with workplace devices to fulfill their tasks. Regardless of the location of these devices (e.g., in the home office), the following rules apply:

- Only devices provided or approved by the COMPANY may be connected to the workplace devices of the COMPANY. Exceptions are input and output devices such as a mouse, keyboard, webcam, headset, and monitor. Devices with which confidential data are input or output must generally be connected with a cable. Exceptions to this rule must be clarified with IT operations, for example, by creating a self-service ticket.
- For the workplace devices of the COMPANY, the principle of a "clear screen" (Clear Screen Policy) applies. This means that the device must be locked when leaving the workplace. Devices used for technical monitoring activities, such as in IT operations, must be protected by other appropriate measures to prevent unauthorized use.
- Configuration or software updates provided by the COMPANY must be installed promptly, considering the necessary availability of the device.
- Writable IT data carriers, such as CDs or DVDs, that are no longer needed must be disposed of in the provided container near the data center entrance.
- When sending confidential documents by fax, the transmission time should be coordinated with the recipient if possible.
- In areas with public traffic, monitors, printers, and fax machines must be positioned to minimize the risk of unauthorized third parties viewing or stealing documents or electronic data carriers (e.g., CD/DVD).
- When using scanners or copiers, the original document must be removed after use. Unattended documents with confidential content or personal data must be submitted to the nearest secretariat.

3.4 Mobile Devices Mobile devices are IT devices that can be operated both inside and outside the COMPANY's premises. These include traditional IT devices such as laptops, as well as more modern devices like smartphones and tablets. For mobile devices of the COMPANY, the following additional regulations apply:

- Data on mobile IT devices must be effectively protected against unauthorized access by third parties, for example, by using passwords or PINs. Access to mobile devices such as smartphones or tablets must be appropriately secured. PINs must be at least four digits long.

- When using mobile devices, especially in public places or at home, it must be ensured that unauthorized persons cannot view confidential or personal data.
- To update the security functions of mobile IT devices, they must be regularly connected to the COMPANY's network. This can be done by connecting the devices to the internal network or establishing a VPN connection. The details, such as how often this should happen, must be regulated and documented when the devices are issued.
- Communication between mobile IT devices and the COMPANY, especially over public networks, must be encrypted. This can be done using encrypted protocols like HTTPS or encrypted network connections like VPN.
- To prevent data loss or unwanted disclosure of internal COMPANY data, data should not be stored on mobile IT devices if possible. If this is unavoidable, the data must be encrypted and otherwise protected from loss.

3.5 Login Procedures Login procedures limit access to IT systems, services, resources, or similar to authorized individuals or groups. It is essential that login data is kept strictly confidential and that items used to establish authorization are not passed on without permission.

3.5.1 Access with "Knowledge" Passwords (or PINs) are examples of login procedures based on secret knowledge - the password. The following general rules apply to password login:

- Passwords must be entered in a way that maintains confidentiality.
- Recording passwords, such as saving them in the browser or writing down a PIN, is generally not allowed. If necessary, other measures must be taken to ensure that passwords are known only to authorized individuals. Linking authentication information to programmable function keys on keyboards or mice is particularly prohibited.
- Passwords must be changed immediately if there is suspicion or risk that unauthorized persons might know them.
- Initial and transitional passwords that may also be known to other individuals must be replaced by individual passwords immediately.

3.5.1.1 Password Conventions In addition to the general rules for knowledge-based login systems (see section 3.5.1), the following rules apply to passwords, provided the technical capabilities exist:

- The password must be at least 15 characters long.
- The password must consist of at least three of the following character groups:
    1. Uppercase letters
    2. Lowercase letters
    3. Numbers

4. Special characters
5. Other characters

- The password must not consist solely of words that a third party might know, such as username, department, last name, first name, season, etc.
- If a procedure for modifying the password is used, the modification rules must only be known to the user.

3.5.2 Access with "Possession" Items like one-time password generators (e.g., RSA tokens) or cryptographic keys (e.g., SSH keys) are examples of login procedures based on possession of an object or data set. The following general rules apply to these login systems:

- The object or data set may only be used personally and must be carried and securely stored for authentication purposes.
- The COMPANY must be informed immediately if the authorized person or group is no longer in possession of the object or data set or if there is suspicion that unauthorized persons might have gained access.

3.6 Software Installations Software may only be installed on the COMPANY's IT devices by individuals explicitly authorized by IT management. Therefore, it is not allowed to install software independently or run software obtained from other sources (e.g., from the internet) without authorization.

3.7 Drives The COMPANY's workplace devices provide two types of drives for file storage:

1. Local drives: These are built into the workplace computer and contain programs and data necessary for the computer's operation. Files on these drives are not centrally backed up.
2. Network drives: These are centrally provided by the COMPANY for storing programs and data. These drives can be used by multiple people depending on access permissions and are backed up daily.

The following general rules apply to using drives:

- Files necessary for the COMPANY's operations must be stored on network drives.
- Files that need to be accessed by other people must be stored on network drives. Appropriate access permissions must be assigned.
- Files with confidential or personal data must be stored so that only authorized persons can access them. Note: The possibility of unauthorized access to confidential data must be reported as a security incident to the "IS-Vorfall" mailbox.

3.7.1 Network Drives The following rules apply to storing files on network drives:

- Drive L: Files related to the organization (e.g., team or department data) must be stored on drive L in the respective organizational area folder.
- Drive N: Files without a clear organizational reference (e.g., project or working group data) must be stored on drive N.
- Drive X: Drive X is provided exclusively for temporary data exchange. Storing confidential company data, such as personal data, signatures, or similar, unencrypted on drive X is prohibited.

3.8 Communication

3.8.1 Emails

Emails with confidential content or classified as "Strictly Confidential" must always be encrypted. Emails classified as "Confidential" or "Internal/Official Use" must be encrypted when sent over public networks, such as the internet. Encryption ensures that only the intended recipients can read the content and that it is transmitted unchanged.

Encryption hints for emails with confidential content:

- To encrypt confidential emails sent only to internal addresses within the COMPANY, use the Notes security function "Encrypt". This ensures that other individuals who have read access to the personal mailbox cannot read the encrypted content.
- For confidential emails sent to external addresses (e.g., internet email addresses), encryption is ensured by sending the content as an encrypted attachment. The password for the attachment must be communicated to the intended recipients preferably through a different communication channel, such as by phone or at least in a separate email.
- To ensure proper receipt, the "Request delivery receipt" option can be used when sending emails. Note: The recipient or their email system may prevent the sending of a delivery receipt.

3.8.2 Conversations

- Confidential conversations, including phone calls, should not be conducted in public places or open offices.
- When conveying confidential information orally to authorized persons, ensure that no unauthorized persons can listen.
- Do not leave confidential information on answering machines or mailboxes.

3.8.3 Web Conferences, Online Seminars, and Presentations

- Participation in online seminars or training must be approved by the respective supervisor in advance.
- Participation in web conferences, online seminars, and presentations using the COMPANY's IT devices is limited to services and applications approved by the COMPANY. Services and applications with remote control functions are prohibited.

- Participation in phone and video conferences and online events (e.g., seminars or training) with private devices is generally allowed. However, their use should be avoided if confidential information is to be exchanged.

3.9 Internet Internet access at the COMPANY is available only for official purposes. The rules are described in the service directive on the use of internet and email at the COMPANY.

3.10 Security Incidents "Information security incidents" are situations that pose a threat to the information security of the company or where the threat has already occurred. Reporting and handling information security incidents is essential to mitigate potential risks and minimize negative impacts. Therefore, it is imperative to report suspected or actual threats promptly via email to "IS-Vorfall". If immediate action is required, additionally report the incident to the reception (extension 333).

Important:

- If there is suspicion of a violation of data protection regulations, report a potential data protection breach immediately (see "GK102.2180P Process for Reporting and Handling Data Breaches" and "GK101.288R Data Protection Policy").
- If there is suspicion of intentional criminal or grossly improper actions, the Internal Audit must also be informed immediately (see "GK101.81L Internal Audit Policy").

Examples of information security incidents include:

- Loss of IT devices
- Significant disruptions of IT applications
- Storage of confidential data in publicly accessible places (e.g., drive X)
- Unauthorized third-party access to secure areas (e.g., IT facilities in the data center)
- Sharing personal passwords or other user accounts
- Violations of internal regulations that could result in security incidents
- Access violations indicating an attempt to misuse rights

4. Entry into Force The revised policy takes effect on October 18, 2023. The previous User Responsibility Policy, version 8.0, dated May 25, 2021, is repealed as of the same date.