Information Security

Security Policy   
Acceptable Use



|  |  |  |
| --- | --- | --- |
|  |  | |
| Acceptable Use Policy | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 02.10.2023 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Topic | Compliance | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last review | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages | English | |
| Formats | Online | |
| Remarks |  | |

Table of contents

[1 Principles 4](#_Toc149123867)

[2 Objectives 4](#_Toc149123868)

[3 Controls 4](#_Toc149123869)

[3.1 General regulations on use and ownership 4](#_Toc149123870)

[3.2 Dealing with visitors 5](#_Toc149123871)

[3.3 Clean Desk and Clear Screen 5](#_Toc149123872)

[3.4 Limited use of devices owned by employees 5](#_Toc149123873)

[3.5 Limited private use of IT services 5](#_Toc149123874)

[3.6 Security and copyrighted information 6](#_Toc149123875)

[3.7 Use of e-mail 6](#_Toc149123876)

[3.8 Use of AI-based tools such as ChatGPT 6](#_Toc149123877)

[3.9 Use of movable electronic data carriers 6](#_Toc149123878)

[3.10 Destruction and disposal of data carriers 7](#_Toc149123879)

[3.11 Unacceptable use or behavior 7](#_Toc149123880)

[3.11.1 General personal behavior 7](#_Toc149123881)

[3.11.2 IT system and network activities 7](#_Toc149123882)

[3.11.3 E-mail and communication activities 9](#_Toc149123883)

[3.11.4 Blogging and social media 9](#_Toc149123884)

# Principles

This guideline defines criteria for the acceptable use of SÜDVERS IT systems and specifies the general information security regulations for end users.

# Objectives

IT systems provide access to data and processes required to support business functions and have contributed to significant improvements in productivity and quality of service for our customers. In order to comply with internal, legal, contractual and other regulations, the use of these IT systems and access to premises where we store or process internal and customer data is subject to rules that must be observed by employees.

# Controls

## General regulations on use and ownership

* Regional, supra-regional, national or foreign or international laws, internal provisions and regulations, agreements or other third-party rights or contractual agreements with customers must be complied with.
* Employees must use SÜDVERS proprietary information and SÜDVERS IT systems and security systems appropriately and in accordance with SÜDVERS policies; internal policies and regulations regarding information security and IT operations must be complied with. The current versions of the information security guidelines are stored in the d3 document archive under the category [Data Protection and Information Security](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/sr/?objectdefinitionids=%5B%22DsIs%22%5D&showdetails=true#searchtemplateroot=history&searchtemplatetitle=Datenschutz%20%26%20Informationssicherheit).
* SÜDVERS' own information stored on electronic devices and computers, regardless of whether they are owned or leased by SÜDVERS, the employee or a third party, shall remain the sole property of SÜDVERS, unless otherwise contractually agreed.
* You are responsible for immediately reporting any inappropriate use, theft, loss or unauthorized disclosure of SÜDVERS proprietary information or IT systems and security systems.
* You may only access, use or disclose proprietary information to the extent permitted and necessary to fulfill the tasks assigned to you.
* Employees are obliged to exercise appropriate care when using the IT systems provided to them and for their storage in order to protect them from damage, destruction or loss.
* Employees are responsible for assessing the appropriateness of personal use to the best of their knowledge and belief and ensuring that private use neither impairs the interests of SÜDVERS nor entails additional obligations for SÜDVERS, such as additional confidentiality, availability or audit requirements, or claims against SÜDVERS (e.g. based on GDPR §17) that would result from the processing of private information. The procedures for evaluating log data must be agreed between the IT department and the company data protection organization. A personal evaluation is carried out exclusively by the data protection officer or his deputy within the framework of the legal requirements. The employee will be informed of the result of the evaluation in writing.
* SÜDVERS reserves the right to inspect networks and systems at regular intervals to ensure compliance with this policy.

## Dealing with visitors

* Visitors must be registered at reception.
* Visitors within the SÜDVERS locations are obliged to wear visible identification during their visit, which clearly identifies them as visitors. Visitor badges must be provided by reception.
* If organizationally possible, visitors are to be accompanied in the buildings.
* The inviting SÜDVERS employee ensures that the visitor passes are returned to reception or signs the visitor out at reception.

## Clean Desk and Clear Screen

* Sensitive information in both physical (paper) and electronic form must be protected against unauthorized access. Further details can be found in the "[Clean Desk and Clear Screen" policy](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P008657591), which is stored in the document archive.

## Limited use of devices owned by employees

* Employees may only use employee-owned IT devices (including tablets and smartphones) for business purposes if the devices in question have been officially approved by SÜDVERS IT and are maintained, managed and operated in accordance with the policy for employee-owned devices. Details can be found in the ["End User Systems" policy](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P008657652), which is stored in the document archive.

## Limited private use of IT systems and IT services

* private use of IT systems and IT services provided by SÜDVERS or on behalf of SÜDVERS (Internet use, use of private electronic communication systems, storage of private data on company IT systems ...) for private purposes is only permitted to the extent that this does not restrict or impair the business interests and / or operational needs of the employer.
* Private use is only permitted to a reasonable extent and in principle only during break times or after business hours and only if and to the extent that this does not impair the fulfillment of business tasks and the availability of IT systems for business purposes.
* The incoming and outgoing emails in the company email inbox are backed up daily to ensure the functionality of the system and stored for a maximum of 10 years. This may also affect private emails, provided they have not been deleted before storage.
* Before leaving the company, the employee must delete his/her personal file, if available. He shall be given a reasonable period of 14 days to do so. If the normal notice periods are observed without a leave of absence, a reasonable period of time is generally given. In the case of leave of absence or resignation without notice, the period will be discussed with the employee. The employer has the right to supervise the use of the SÜDVERS systems during this period, taking into account the interests of both parties.

## Security and copyrighted information

* Information must be classified and protected according to its criticality classification. Further information can be found in the [guideline "Information Classification](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P008657659)", which is stored in the d3 document archive.
* All mobile devices and computers connected to the internal network must comply with the End User Device Policy.
* The passwords at system and user level must comply with the ["Passwords" guideline](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P008657655). It is prohibited to grant access to another person, either intentionally or because access has not been secured.
* All personal computing devices must be secured with a password-protected screensaver configured according to the password policy.
* Contributions by employees posted to newsgroups or other social media from a SÜDVERS email address must include a disclaimer stating that the opinions expressed are solely their own and not necessarily those of SÜDVERS, unless the contribution is made in the course of business duties.
* Employees must be extremely careful when opening email attachments that come from unknown senders and may contain malware.

## Use of e-mail

* E-mail is one of the standard communication systems for SÜDVERS' internal business communication as well as for the exchange of information with our customers, and SÜDVERS allows limited private use of these systems ([see chapter Limited private use of IT services](#_Begrenzte_private_Nutzung)). Consequently, the use of e-mail must be regulated appropriately. Further information on the use of e-mail can be found in the ["E-mail" policy](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P008657580), which is stored in the d3 document management system.

## Use of AI-based tools such as ChatGPT

* The use of AILLM tools, such as ChatGPT, offers SÜDVERS considerable potential for optimizing and increasing the efficiency of its services. However, in order to comply with the legal requirements regarding the use of information, to protect the legitimate interests of our customers and to protect SÜDVERS business information, it is essential that some basic rules regarding the use of these tools are observed. Further information regarding the use of AILLM tools can be found in the [guideline "Usage of Artificial Intelligence Based Large Language Models](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P009234830)", which is stored in the d3 document management system.

## Use of movable electronic data carriers

* Portable electronic data carriers (e.g. USB sticks) are used for a wide variety of purposes: to start portable software and entire operating systems as well as to back up or transport data. The use of such storage media is generally prohibited; regulations for exceptional cases can be found in the corresponding directive. If an exception applies, the data on these must be protected in accordance with the SÜDVERS guidelines. Details on this can be found in the ["Portable IT storage media" policy](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P008657594), which is stored in the document archive.

## Destruction and disposal of data carriers

Information that is stored on data carriers (e.g. paper, computer hard disk, smartphone, etc.) must be securely deleted or disposed of if it is no longer required or if there is no longer a legal basis (e.g. in accordance with the requirements of the GDPR for personal data) for its storage. Further information can be found in the ["Destruction and disposal of data carriers" guideline](https://svg-ecm.d-velop.cloud/dms/r/0e257714-036e-558c-9925-06f4788f50d0/o2/P008657587), which is stored in the d3 document archive.

## Unacceptable use or behavior

The following activities are generally prohibited. Employees may be exempt from these restrictions as part of their lawful duties (e.g., system administration employees may be required to disable a host's network access if that host interferes with production services). Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law. The lists below are by no means exhaustive, but are intended to provide a framework for activities that fall into the category of unacceptable use.

### General personal behavior

The following activities are prohibited without exception:

* Violations of regional, supra-regional, national or foreign or international laws, internal provisions and regulations, agreements or other third-party rights or contractual agreements with customers
* Disclosure of confidential SÜDVERS information in conversation with people in public places (café, street, airplane, train...)
* Disclosure of information about others or of specific information that is of significant value to SÜDVERS and which must not be disclosed to the wrong persons
* If you use a SÜDVERS mobile device to access SÜDVERS data in public places without paying attention to your surroundings and ensuring that your device is not viewed or "spied on" by unwanted persons
* Stealing confidential SÜDVERS information, SÜDVERS software or SÜDVERS devices without prior (implicit or explicit) authorization.

### IT system and network activities

The following activities are prohibited without exception:

* Violation of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property or similar SÜDVERS or regulation, including but not limited to the installation or distribution of "pirated" or other software products that are not properly licensed for use by SÜDVERS.
* Unauthorized copying of copyrighted material, including but not limited to digitizing and distributing photographs from magazines, books or other copyrighted sources, copyrighted music, and installing copyrighted software for which the end user does not have an active license is strictly prohibited.
* The export of software, technical information, encryption software or technology that violates SÜDVERS international or regional export controls is illegal. The responsible line organization must be consulted prior to the export of materials in question.
* Execution of activities directed against the security of IT systems (e.g. attacks on external web servers)
* Retrieval of Internet pages for which SÜDVERS is liable to pay costs,
* Sharing your account password with others or allowing others to use your account.
* Storage of authentication data (user name or password) on computers that do not belong to SÜDVERS (e.g. if the browser asks you to remember your access data).
* Removal of restrictions on your SÜDVERS smartphone for downloading additional applications that are not available in the official Apple Store and Play Store (jailbreaking for iOS or rooting for Android)
* Use of a computer to obtain, store, process or transmit information/content that violates SÜDVERS regulations or legal regulations in the area of application of the user's location.
* Distributing fraudulent offers of products, items or services originating from any account.
* Making express or implied warranties, unless this is part of normal professional duties.
* Causing security breaches or disruptions to IT systems. Security breaches include, but are not limited to, accessing data for which the employee is not the intended recipient or logging into a server or account that you are not expressly authorized to do, unless these tasks are part of your regular duties.
* Any form of network monitoring, unless this activity is part of your normal work/duty.
* Bypassing user authentication or the security of a computer, network or user account.
* Enable peer-to-peer file sharing on your computer or mobile device.
* Impairment or denial of services for other users (e.g. denial of service attack).
* Disclosure of information about or lists of employees to parties outside SÜDVERS.

### E-mail and communication activities

When using company resources to access the internet or send emails, users must be aware that they are representing the company. If employees indicate an affiliation with the company, they must clearly indicate, unless authorized to do so, that "the opinions expressed are his or her own and not necessarily those of the company". Questions in this regard can be directed to the HR department.

The following are prohibited in this context

* Sending unsolicited e-mail messages, including sending "junk mail" or other advertising material to persons who have not expressly requested such material (e-mail spam).
* Any form of harassment by e-mail, telephone or paging, whether by language, frequency or volume of messages.
* Unauthorized use or falsification of e-mail header data.
* Sending emails with the intention of harassing people or collecting responses
* Creation or forwarding of "chain letters", "Ponzi" or other "snowball systems" of any kind.
* Posting the same or similar non-business related messages to a large number of Usenet newsgroups (newsgroup spam).
* Sending information classified as "internal" or higher by e-mail without applying appropriate safeguards in accordance with the Information Classification Policy.
* Forwarding e-mails to non-SÜDVERS e-mail accounts, unless this has been expressly authorized by your superior.
* Sending e-mails with content that is contrary to the business interests of SÜDVERS.
* Replying to SPAM or unsubscribing from "unsolicited" e-mail distribution lists, as this confirms a valid recipient

### Blogging and social media

* Blogging by employees, whether using SÜDVERS property and systems or personal computer systems, is also subject to the conditions and restrictions set out in this policy. Limited and occasional use of SÜDVERS' systems for blogging is acceptable, provided it is done in a professional and responsible manner, does not violate SÜDVERS' policies, is not detrimental to SÜDVERS' interests, and does not interfere with the employee's regular job duties. Blogging on SÜDVERS' systems is also subject to monitoring.
* SÜDVERS' Information Classification Policy also applies to blogging. Therefore, employees are prohibited from disclosing confidential or proprietary information, trade secrets or other material covered by SÜDVERS' Information Classification Policy when blogging.
* Employees may not participate in blogs that could damage or impair the image or reputation of SÜDVERS and/or its employees. Employees are also prohibited from making discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in conduct prohibited by SÜDVERS.
* Employees may also not express personal statements, opinions or beliefs when blogging. When an employee expresses his or her beliefs and/or opinions in blogs, he or she may not represent himself or herself as an employee or representative of SÜDVERS, either explicitly or implicitly. Employees bear all risk associated with blogging.
* Apart from complying with all SÜDVERS regulations on handling copyrighted or export-controlled material, trademarks, logos and other intellectual property of SÜDVERS may not be used in connection with blogging activities.