

Security Policy   
Clean Desk and Clear Screen

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Security Policy Clean Desk and Clear Screen | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | ChiefInformation Security Officer | |
| Entry into force | 04.07.2022 | |
| 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 | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Table of contents

[1 Principles 4](#_Toc187740087)

[2 Goals 4](#_Toc187740088)

[3 Controls 4](#_Toc187740089)

[3.1 Technical or infrastructure-related controls: 4](#_Toc187740090)

[3.2 User-related controls: 4](#_Toc187740091)

[3.2.1 Additional user-related requirements for open office spaces, offices for several employees and meeting rooms 5](#_Toc187740092)

# Principles

Information that requires a special level of protection beyond the normal level of information we deal with within SÜDVERS (i.e. information classified as "Restricted" and above) must be protected by additional controls against unauthorized access by internal or external persons. In addition, the meeting rooms we use require some specific controls to ensure that both security and operational aspects are covered.

# Goals

Reduce the risk of unauthorized access to, loss of and damage to information on desks, screens and other accessible locations during and outside regular working hours.

# Controls

## Technical or infrastructure-related controls:

* Information must be protected in accordance with the relevant legal requirements (e.g. encryption of information covered by the Data Protection Act) and in accordance with SÜDVERS' Information Classification Policy.
* Building management must ensure that suitable facilities are available in the office buildings in which computer media and paper and file folders can be stored and locked away, depending on the security classification, including in lockable containers, filing cabinets and cupboards
* The IT helpdesk must ensure that all IT systems that are technically capable of doing so are protected by password-protected screensavers that automatically become active after a maximum of 15 minutes of inactivity
* The IT helpdesk must provide users with intelligent screen filters on request, which enable them to protect the screen content of their devices from being viewed by unwanted persons
* Incoming and outgoing mail collection points and fax systems must be protected or monitored to ensure compliance with regulatory requirements and to prevent information from being stolen or lost
* Photocopiers, scanners and multifunctional devices used for printing non-public information may only be set up in protected areas.

## User-related controls:

* Information must be protected in accordance with the relevant legal requirements (e.g. paper copies containing information covered by the Data Protection Act must be locked away when not in use).
* Information that requires a higher level of protection than "internal" must be securely locked when not in use (e.g. in lockable containers, filing cabinets or cupboards, locked rooms). Outside business hours, a locked room is not considered sufficient for information above the "restricted" classification level.
* Personal IT systems must be protected by screen savers when they are unattended
* Personal IT systems must be switched off when not in use and must be protected by password-protected screensavers during normal working hours.
* Personal IT systems must be positioned in such a way that unintentional disclosure of the information displayed is avoided (e.g. by not allowing the screen to be seen through a window from outside the room ...)
* Users must log out of their personal IT devices as soon as they no longer need to be logged in.
* Users must lock their screens if they leave their computers unattended.
* Users must use smart screen filters on their devices when working with confidential information in public areas.
* Printouts on printers, scanners, fax machines and multifunction devices must be removed promptly

### Additional user-related requirements for open office spaces, offices for several employees and meeting rooms

* Information that requires a higher level of protection than "internal" must be deleted from whiteboards and other display devices when leaving the rooms
* Tables, whiteboards, flipcharts... must be tidied up when leaving the office or meeting room and sensitive information must not be made accessible to others.