

Security Policy   
Physical and Environmental Security

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Physical and Environmental Security | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information 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 Content

[1 Principle 4](#_Toc187839110)

[2 Objective 4](#_Toc187839111)

[3 Controls 4](#_Toc187839112)

[3.1 Physical security perimeter 4](#_Toc187839113)

[3.2 Physical access 5](#_Toc187839114)

[3.3 Physical security monitoring 6](#_Toc187839115)

[3.4 Power supplies 6](#_Toc187839116)

[3.5 Protection against physical and environmental threats 7](#_Toc187839117)

[3.6 Physical protection of IT facilities, outside the SÜDVERS premises 7](#_Toc187839118)

# Principle

All internal IT facilities (including locations where computer systems such as data centers, networks, telecommunications equipment, sensitive physical material and other critical assets are located) must be physically protected against accidents, unauthorized physical access, power outages, fire, flood, environmental and other natural hazards.

# Objective

Restricting physical access to authorized persons, ensuring that central IT equipment is available when needed, and preventing disruption of critical services due to loss or damage to equipment or facilities, power failure, and damage due to fire, flood and other types of hazards.

# Controls

## Physical security perimeter

A physically solid perimeter must be created for a building or site containing information processing facilities (i.e. there should be no gaps in the perimeter or areas through which it is easy to break in). The external roofs, walls, ceilings and floors of the premises must be solidly constructed and all external doors must be suitably protected against unauthorized access by means of control mechanisms (e.g. grilles, alarms, locks). Doors and windows must be locked when unattended and consideration should be given to external protection for windows, particularly on the first floor; ventilation points should also be considered.

Buildings housing internal IT facilities (including SÜDVERS office buildings) must be protected against unauthorized access by providing the following measures:

* Provide locks, bolts (or similar) on vulnerable doors and windows
* Installation of burglar alarms on accessible external doors and windows and their regular inspection.

Internal IT facilities (including within SÜDVERS' office buildings) must be protected by not being publicly accessible and by keeping their data confidential (e.g. through discreet signage and exclusion of data from directories or telephone directories).

## Physical access

Physical access to central IT facilities (data centers, including in SÜDVERS office buildings) must be protected by:

* Definition and reinforcement of physical security boundaries (e.g. solid walls, alarm-protected fire doors, armored windows and physical barriers)
* Constant monitoring of the buildings
* Installation of video surveillance systems (CCTV) or equivalent equipment
* Placement of computer equipment (e.g. server console screens, computers and printers) so that sensitive information cannot be viewed.

Physical access to internal IT facilities (including within SÜDVERS office buildings) must be restricted to authorized persons by

* Lock doors/windows when leaving the area
* Installation of burglar alarms
* staff are obliged to check unknown persons

Physical access to critical IT facilities (including SÜDVERS' office buildings) (including those that support or enable SÜDVERS' critical infrastructure) must be restricted to authorized individuals by:

* access control systems activated by keypads, magnetic cards or equivalent means are used
* Doors/windows are locked when leaving the area
* Burglar alarms are installed and activated
* personnel is obliged to check unknown persons

Authorization for physical access to internal IT facilities (including SÜDVERS office buildings) must:

* are issued in accordance with documented standards/procedures
* are regularly reviewed to ensure that only suitable persons are granted access
* be revoked immediately if they are no longer required.

External visitors to internal IT facilities (including those in SÜDVERS office buildings) must:

* to grant access only for specified and authorized purposes
* monitored by recording arrival and departure times
* Receive instructions explaining the safety requirements of the area, describing emergency procedures and stating that audio and other recordings are prohibited
* obliged to return all physical access mechanisms when they are no longer required.

Persons should be required to obtain authorization before leaving SÜDVERS premises with IT equipment (such as servers, network devices, printers and special equipment).

## Physical security monitoring

The physical premises must be monitored by surveillance systems, which may include security guards, intruder alarms, video surveillance systems such as video inspection systems and physical security information management software, either managed in-house or by a surveillance service provider.

Access to buildings in which critical IT systems are located must be constantly monitored by the following means in order to detect unauthorized access or suspicious behavior by persons:

* Installation of video surveillance systems, such as video inspection systems, to monitor and record access to sensitive areas inside and outside an organization's premises;
* Installation of contact, sound or motion detectors that trigger an intruder alarm in accordance with the relevant applicable standards and their regular testing,

The surveillance systems must be protected against unauthorized access in order to prevent unauthorized persons from accessing surveillance data, such as video images, or to prevent systems from being deactivated remotely.

## Power supplies

The power supply of the internal IT facilities (including those of the SÜDVERS office buildings) must be protected by uninterruptible power supply (UPS) devices which, if necessary

* have a battery capacity that enables an orderly shutdown of IT systems and supporting systems
* be maintained in accordance with the manufacturer's recommendations
* be tested regularly (at least every 6 months).

Fire detectors (smoke detectors) must be continuously monitored, regularly tested and maintained in accordance with the manufacturer's instructions.

## Protection against physical and environmental threats

Buildings housing central IT facilities (including SÜDVERS' office buildings) must be protected from environmental hazards by locating them geographically in areas with non-significant risks.

Critical IT equipment (e.g. server rooms) must be housed in a secure environment and in rooms that:

* are built with fireproof materials for walls, doors, windows and furniture
* are free from inherent fire hazards (e.g. flammable paper or flammable chemicals)
* are equipped with fire alarm systems (e.g. with a combination of smoke detectors, optical detectors and temperature sensors)
* are protected with fire extinguishing systems (e.g. with water, carbon dioxide or FM-200 extinguishing systems)
* provide protection against natural hazards (e.g. storm and flood damage).

Fire alarms must be constantly monitored, regularly tested and maintained in accordance with the manufacturer's instructions.

The effects of hazards must be minimized by:

* Placement of portable fire extinguishers so that minor incidents can be tackled without delay
* Training staff in the use of fire extinguishers and other emergency/safety equipment and in evacuation procedures
* Conducting fire drills so that employees know how to leave SÜDVERS premises safely
* Protection of IT equipment against damage caused by environmental influences (e.g. smoke, dust, vibrations, chemicals, electrical interference/radiation, food, drinks)
* Monitoring and control of temperature and humidity in data centers and computer rooms (or equivalent) in accordance with equipment manufacturers' recommendations.

## Physical protection of IT facilities, outside the SÜDVERS premises

Physical access to IT facilities must be restricted to authorized persons by:

* Storage in locked cabinets or in environments to which access is controlled by SÜDVERS is guaranteed.