

Security Policy   
Asset management

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Asset Management | |  |
| Number | [Number] | |
| Issued on | 01.03.2025 | |
| Through | Chief Information Security Officer | |
| Entry into force | 01.07.2025 | |
| 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](#_Toc188257129)

[2 Goals 4](#_Toc188257130)

[3 Controls 4](#_Toc188257131)

[3.1 Asset Register 5](#_Toc188257132)

[3.1.1 Register of IT assets 5](#_Toc188257133)

[3.1.2 Register of business information 5](#_Toc188257134)

[3.2 Return of assets 6](#_Toc188257135)

# Principles

All business information and other related assets must be identified and their significance in terms of information security determined. The documentation must be stored appropriately in the company's own or existing asset registers.

# Goals

Identify the organization's information and other related assets to maintain their information security and assign appropriate responsibilities

# Controls

The inventory of information and other related assets must be complete, accurate, current, consistent and reconciled with other inventories. Ensuring the accuracy of the inventory of information and other related assets includes

* Conduct regular reviews of the identified information and other related assets based on the inventory of assets;
* Automatically force an inventory update when an asset is installed, modified or removed.

The owner of an asset is responsible for the proper management of that asset throughout its lifecycle and must ensure that:

* information, IT assets and other related assets are inventoried;
* information, IT assets and other related assets are appropriately classified and protected;
* the classification is reviewed periodically;
* components to support technology values are listed and linked together, e.g. database, memory, software components and subcomponents;
* requirements for the permitted use of information and other related assets;
* the access restrictions comply with the classification, are effective and are reviewed regularly, at least annually;
* Information and other related assets, when deleted or disposed of, are handled in a secure manner and removed from the inventory;
* he is involved in the identification and management of the risks associated with his asset(s);
* it supports the employees who have the task and responsibility of managing the respective assets.

## Asset Register

### Register of IT assets

Registers of IT assets must be created and maintained. At least the following information must be included:

* Unique identifier (can be: Inventory number (would be preferred, ideally with RFID tags or a corresponding barcode-readable asset tag), serial number, ...)
* Categorization of the asset (hardware, software, ...)
* Name of the IT system
* Description
* Intended use
* Manufacturer
* Model designation
* Version
* Location
* IP address (if permanently assigned, otherwise reference to dynamic IP via DHCP, ...)
* MAC address
* Asset owner (legally speaking, who formally owns the device, this can be the responsible Südvers company, for example)
* Asset owner (the person who normally owns the device, for laptops this would usually be the user)
* Responsible role/person in IT for the configuration of the device
* Criticality classification (for realistic and worst-case scenarios. Levels: negligible, low, medium, high) of the asset (based on the criticality analysis performed) in relation to
  + Confidentiality
  + Integrity of the stored/processed data
  + Availability

### Register of business information

Registers of business information must be created and maintained. At least the following information must be included:

* Business information
* Information owner
* Information manager
* Criticality classification (for realistic and worst-case scenarios. Levels: negligible, low, medium, high) of the asset (based on the criticality analysis performed) in relation to
  + Confidentiality
  + Integrity of the stored/processed data
  + Availability
* List of IT systems on which the business information is processed and/or stored
* List of non-IT systems (e.g. paper filing system, archive, ...) on which the business information is stored

## Return of assets

The HR SML process must be formalized to include the return of all previously issued physical and electronic assets owned by SÜDVERS or entrusted to SÜDVERS for safekeeping or use. In cases where employees and other interested parties who acquire SÜDVERS equipment or use their own equipment, procedures shall be defined and followed to ensure that all relevant information is traced and transmitted to SÜDVERS and securely deleted from the equipment.

In cases where personnel and other interested parties have knowledge that is important for ongoing operations, this information must be documented by the respective managers and submitted to the responsible SÜDVVERS department. All information to be returned and other related assets must be identified and documented, including (but not limited to)

* User devices (cell phones, laptops, printers, monitors, keyboards, mice, ...);
* portable storage devices;
* authentication hardware (e.g. mechanical keys, physical tokens and smart cards) for information systems, sites and physical archives; e) physical copies of information.
* Other IT hardware