

Security Policy   
Capacity management

Information security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Capacity 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 review | 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](#_Toc194566586)

[2 Goals 4](#_Toc194566587)

[3 Controls 4](#_Toc194566588)

# Principles

The capacity requirements for information processing systems, personnel capacities, offices and other facilities must be determined taking into account the criticality of the affected systems and processes, the IT systems must be monitored with regard to these and, if necessary, measures must be initiated to ensure and, if necessary, improve the availability of the systems.

# Goals

Ensure that hardware, software, services and networks function correctly with the required security settings and that the configuration is not altered by unauthorized or incorrect changes.

# Controls

The capacity requirements for information processing equipment, staff capacity, offices and other facilities should be determined taking into account the criticality of the systems and processes concerned. The system should be coordinated and monitored in order to ensure and, if necessary, improve the availability of the systems.

SÜDVERS should (for important and critical IT services must) perform stress tests of systems and services to confirm that sufficient system capacity is available to meet peak performance requirements.

Detective measures should be put in place (for important and critical IT services) to identify problems in good time. Forecasts of future capacity requirements should take into account new business and system requirements as well as current and future trends in the organization's information processing facilities.

Particular attention should be paid to resources with long procurement lead times or high costs. Therefore, managers, service or product owners should monitor the utilization of key system resources.

The provision of sufficient capacity can be achieved by increasing capacity or reducing demand. To increase capacity, the following should be considered:

* Recruitment of new staff;
* the procurement of new facilities or premises;
* the acquisition of more powerful processing systems, memory and storage;
* d) the use of cloud computing, whose inherent characteristics directly address the capacity issue. Cloud computing has elasticity and scalability that make it possible to quickly expand or reduce the resources available for certain applications and services as required.

The following points should be considered to reduce the demand on the organization's resources:

* Deletion of obsolete data (storage space);
* Disposal of paper documents whose retention period has expired (freeing up shelf space);
* Decommissioning of applications, systems, databases or environments;
* Optimization of batch processes and planning;
* Optimization of application code or database queries; f) Denial or limitation of bandwidth for resource-intensive services that are not critical (e.g. video streaming).