

Security Policy   
Configuration management

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Configuration 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](#_Toc187920026)

[2 Goals 4](#_Toc187920027)

[3 Controls 4](#_Toc187920028)

[3.1 Standard templates 4](#_Toc187920029)

[3.2 Management of configurations 4](#_Toc187920030)

[3.3 Monitoring of configurations 5](#_Toc187920031)

# 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

## Standard templates

Standard templates must be defined for the secure configuration of hardware, software, services and networks.

When creating standard templates for the secure configuration of hardware, software, services and networks, at least the following points must be taken into account:

* Minimize the number of identities with privileged or administrative access rights;
* Deactivation of unnecessary, unused or insecure identities;
* Deactivation or restriction of functions and services that are not required;
* Restrict access to powerful utilities and host parameter settings;
* Synchronization of the clocks;
* Changing the manufacturer's default authentication data, such as default passwords, immediately after installation and checking other important security-relevant default parameters;
* Calling up timeout facilities that automatically log off computer devices after a certain period of inactivity;
* Check whether the license requirements are met

The templates should be regularly reviewed and updated when new threats or vulnerabilities need to be addressed or when new software or hardware versions are introduced.

## Management of configurations

Existing configurations of hardware, software, services and networks must be documented and changes to these must be logged.

Changes to configurations are subject to the change management process.

## Monitoring of configurations

The configurations must be monitored and regularly checked using a comprehensive set of system management tools (e.g. maintenance programs, remote support, enterprise management tools, backup and recovery software) in order to verify the configuration settings, evaluate the password strength and assess the activities performed. Actual configurations must be compared with the defined target templates and deviations must be responded to by either automatically enforcing the defined target configuration or manually analyzing the deviation and taking corrective action.