

Security Policy   
Network storage systems

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Network storage systems directive | |  |
| 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 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 Principle 4](#_Toc107921038)

[2 Objective 4](#_Toc107921039)

[3 Controls 4](#_Toc107921040)

# Principle

Network storage systems must be protected by system and network controls.

# Objective

Ensure that network storage systems function as intended, are available when required and do not jeopardize the security of stored information.

# Controls

Network storage systems, such as Storage Area Network (SAN) and Network Attached Storage (NAS), must be deployed, configured and maintained in accordance with documented IT standards/procedures.

The IT standards/procedures must cover the following

* Design and configuration of network storage systems
* Implementation of standard security practices (e.g. configuration, malware protection, change management and patch management)
* Protection of network storage management consoles and management interfaces
* Encryption of sensitive information stored on network storage systems
* specific security precautions for NAS and SAN.

Network storage systems must be subject to standard security management practices, including

* Restriction of physical access,
* System hardening,
* Change management and protection against malware,
* their monitoring and
* regular checks.

The components of network storage systems (including operating systems, SAN switches and management consoles as well as operating systems and utilities for NAS devices) must be protected as follows

* Restrict administrator access (e.g. to SAN management consoles and utilities for NAS devices) to a limited number of authorized employees (e.g. storage administrators)
* the use of access controls that support individual accountability and prevent unauthorized access
* Restriction of management functions (e.g. in SAN management consoles and NAS device utilities)
* Use of secure web protocols and secure services such as TLS, IPsec or equivalent for accessing the management console and SSH for running terminal sessions.