

Security Policy   
Hardening of IT systems

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Guideline Hardening of IT systems | |  |
| 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 contents

[1 End user systems: 4](#_Toc187664233)

[2 Server systems 4](#_Toc187664234)

[3 Network and firewall components 5](#_Toc187664235)

[4 Other systems: 5](#_Toc187664236)

SÜDVERS defines the minimum hardening standards to be complied with for its IT systems and security systems as described below. For IT systems and security systems that are not listed in this document, the security and hardening recommendations of the respective manufacturers apply as binding hardening standards.

Unless otherwise stated, level 1 of the standards listed below is considered an appropriate general minimum level of protection. For systems that fall below level "high" according to the criticality analysis, it is recommended to increase the level to 2.

Before applying the hardening standards, their compatibility with the business requirements must be checked; any necessary deviations from the standards must be documented.

# End user systems:

For laptops, tablets and smartphones, the CIS hardening standards apply in the latest or penultimate version for operating systems, Internet browsers and Office applications.

If the manufacturer's hardening recommendations or the data protection recommendations of the BSI contradict the requirements of the CIS standard, it must be determined on a case-by-case basis which of the settings should be used for SÜDVERS.

The respective standards can be accessed via the following link: [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/)

If no CIS hardening standard is available for the IT system used, the respective hardening standard of the respective manufacturer shall be applied, if available; if this does not exist either, another hardening standard recognized as best practice for this IT system shall be applied, if available; if these do not exist either, a hardening standard available for comparable IT systems shall be adapted and used

# Server systems

For server systems, the CIS hardening standards apply in the latest or penultimate version for operating systems and server applications.

If the manufacturer's hardening recommendations or the data protection recommendations of the BSI contradict the requirements of the CIS standard, it must be determined on a case-by-case basis which of the settings should be used for SÜDVERS

The respective standards can be accessed via the following link: [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/)

If no CIS hardening standard is available for the IT system used, the respective hardening standard of the respective manufacturer shall be applied, if available; if this does not exist either, another hardening standard recognized as best practice shall be applied for this IT system, if available; if these do not exist either, a hardening standard available for comparable IT systems shall be adapted and used.

# Network and firewall components

For firewalls and network components, the latest or penultimate version of the CIS hardening standards apply.

If the manufacturer's hardening recommendations or the data protection recommendations of the BSI contradict the requirements of the CIS standard, it must be determined on a case-by-case basis which of the settings should be used for SÜDVERS

The respective standards can be accessed via the following link: [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/)

If no CIS hardening standard is available for the IT system used, the respective hardening standard of the respective manufacturer shall be applied, if available; if this does not exist either, another hardening standard recognized as best practice for this IT system shall be applied, if available; if these do not exist either, a hardening standard available for comparable IT systems shall be adapted and used.

# Other systems:

The curing standards in the respective specified or newer available version apply:

* CIS Benchmark for MS Azure Foundations V.3.0.0
* CIS Benchmarks for Microsoft 365 Foundations V.3.1.0
* CIS Microsoft Intune for Windows Benchmark v3.0.1
* CIS Microsoft Intune for Windows Office v1.1.0
* CIS Benchmark for Docker: [CIS Docker Benchmarks](https://www.cisecurity.org/benchmark/docker)
* CIS Kubernetes Benchmark: [CIS Kubernetes Benchmarks](https://www.cisecurity.org/benchmark/kubernetes)
* CIS Multi-Function Device Benchmark v1.0.0

If the manufacturer's hardening recommendations or the data protection recommendations of the BSI contradict the requirements of the CIS standard, it must be determined on a case-by-case basis which of the settings should be used for SÜDVERS

The respective standards can be accessed via the following link: [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/)

If no CIS hardening standard is available for the IT system used, the respective hardening standard of the respective manufacturer must be applied, if available; if this does not exist either, another hardening standard recognized as best practice for this IT system must be applied, if available; if these do not exist either , a hardening standard available for comparable IT systems must be adapted and used.