

Security Policy   
Performance Monitoring

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Directive Performance Monitoring | |  |
| 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, its majority-owned subsidiaries, and 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](#_Toc107911880)

[2 Objective 4](#_Toc107911881)

[3 Controls 4](#_Toc107911882)

# Principle

The performance of business applications, IT systems and networks must be continuously monitored and checked by the IT system managers.

# Objective

Reducing the likelihood that reduced system performance or unavailability will have a negative impact on business operations

# Controls

The performance of business applications, IT systems and networks must (as far as technically possible and economically justifiable) be

* based on agreed targets,
* by checking the current utilization of the systems at normal and peak times,
* with the help of automatic monitoring software that generates alerts based on predefined threshold values
* by regularly checking event logs of system and network activity, and
* through the investigation of bottlenecks/overloads

be monitored.

When planning capacity, the requirements for system criticality (based on the criticality analyses carried out) must be taken into account.

Information related to system/network monitoring must be retained long enough to meet legal/regulatory requirements.

System/network availability (e.g. response and uptime) should be measured from the user's perspective (e.g. by monitoring the performance of information systems and networks).

Capacity planning must be carried out so that additional capacity can be provided before the predicted bottlenecks/overloads occur.

The results of the monitoring measures must be reviewed by the IT system managers and should be made available to the specialist departments for which the services are provided.