

Security Policy   
Change Management

Information security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Change Management | |  |
| 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 | 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 Content

[1 Principle 4](#_Toc107986230)

[2 Objective 4](#_Toc107986231)

[3 Controls 4](#_Toc107986232)

# Principle

Changes to business applications, information systems and network devices must be approved, tested, reviewed and implemented as part of a change management process.

# Objective

Ensure that changes are made correctly and do not jeopardize the security of business applications, computer systems or networks.

# Controls

A management process based on internationally recognized service management standards must be defined and implemented that meets regulatory requirements and covers all types of changes, including

* Upgrades and changes to
* Business applications
* Hardware and software in general
* Emergency corrections and
* Changes to information systems and networks

The change management process must be documented and include the approval and review of changes to ensure that:

* that they are carried out correctly, safely and reliably
* they do not compromise information security and/or data protection requirements
* they do not have a negative impact on the intended services
* no unauthorized changes have been made

Before changes are made in the live environment, they must be:

* be documented
* the interested parties concerned are informed of the intended changes before they are implemented
* be approved by the role designated in the change management process.
* the potential impact of the changes on the business is assessed
* tested to ensure that the system works as intended
* checked to ensure that they do not interfere with security controls
* are checked to ensure that they do not violate existing compliance and legal regulations (e.g. GDPR or EU Regulation 2022/2554).
* Back-out positions are set up so that IT systems and networks can be restored in the event of failed changes or unexpected results.

Changes to information systems and networks must:

* are carried out by qualified and competent persons who are able to make changes correctly, safely and reliably
* be reviewed by the role designated in the change management process and its correct implementation confirmed

Precautions must be taken to ensure that after changes have been made:

* version control is updated (e.g. through configuration management)
* documentation is kept that shows
  + what has been changed
  + when, and
  + by whom
* the responsible persons are informed about the changes made
* to confirm that only the intended changes have been made, checks are carried out
* the documents associated with the information systems and networks are updated (e.g. inventory, design information, system configuration, implementation details and records of all changes to information systems and networks)
* the IT-BCM plans are updated if necessary
* the classification of information in connection with information systems and networks is reviewed and updated if necessary
* secure standard configurations (such as server images and standard builds) are updated to ensure that the changes also apply to new builds