

Security Policy   
Backups of information

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Backups of information | |  |
| Number | [Number] | |
| Issued on | 21.01.2025 | |
| Through | Chief Information Security Officer | |
| Entry into force | 01.07.2025 | |
| 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 | Data backup policy | |
| 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 Principle 4](#_Toc107911880)

[2 Objective 4](#_Toc107911881)

[3 Controls 4](#_Toc107911882)

# Principle

Backups of important information and software must be carried out regularly and according to a defined cycle to enable recovery.

# Objective

Ensure that all essential information or software can be restored within a defined critical time frame in the event of an emergency.

# Controls

Backups of essential information and software (e.g. business information, system information and application information) must be performed frequently enough to meet business requirements. The minimum requirements can be found in the respective BIAs.

Backups must be stored in such a way that the failure of the primary location of the IT systems cannot lead to the unavailability of the backups. (e.g. by storing the backups in a remote second data center)

IT must have documented standards/procedures for performing backups that cover at least the following

* the business requirements for performing backups
* the persons responsible for data backups
* Methods for performing data backups (including validation, labeling and storage)
* the technology used
* Backup cycles (how often and when)
* Number of generations to be stored
* Backup media to be used
* Location of the storage media
* Specifications regarding the protection of backup copies (including access control and cryptography)
* Requirements for the transportation of media, if necessary

The backup arrangements must be based on the identification of critical periods for the recovery of information, taking into account at least the following

* the type of information to be backed up and the location where it is stored
* Legal, regulatory and contractual requirements (e.g. handling of personal data, storage of documents and customer information)
* Business continuity plans and related agreements
* RTO requirements
* RPO requirements
* Interdependencies between the systems (e.g. restoring access control information in one system can lead to inconsistencies in other systems)

Backup arrangements must enable the recovery of operating systems, application software, system software related to technical infrastructure (e.g. computer equipment, virtual systems, network equipment and critical infrastructure) and business information within a critical timeframe by utilizing the following

* Online storage, which usually enables almost immediate access to the backup copies of the information
* Nearline storage that enables information to be restored within minutes
* Offline storage, which can often lead to longer recovery times

Backups must:

* be carried out with special backup management software to increase the security of the backed-up information
* recorded in a log containing details of the data backed up, the date and time of the backup, an expiry date for the backup, the backup medium used and its physical location
* to ensure that backed-up software and information can be successfully restored. At least annual recovery tests must be carried out for the respective IT system environments.
* be associated with control points in live processes (e.g. through the use of timestamps)
* Comparison with the live version when copies are created (e.g. by checking the file size, using hash sums or other verification methods)
* are clearly and precisely labeled
* be protected against accidental overwriting and subject to the same level of protection as the original data

Backups must be protected against loss, damage and unauthorized access, whereby at least the following requirements must be met:

* Storage of the backup media in accordance with the manufacturer's instructions
* For portable storage media: storage in a locked, fireproof computer safe at the data recovery site so that important information can be recovered quickly
* Keep copies off-site in secure facilities at a suitable distance to allow recovery of systems or networks via alternative facilities in the event of a disaster
* Restrict access to a limited number of authorized persons (e.g. through the use of access control software, physical locks and keys)

Backups must be encrypted in order to protect sensitive information if this:

* transferred to backup media to prevent unauthorized interception
* stored on movable media (to prevent unauthorized access if the backup media is stolen or lost on the way to another location, e.g. an external storage facility)

In addition to data backup, IT must define the following documented standards/procedures for recovery:

* Operating processes for recovery
* Recovery time

Backup and restore jobs must be monitored by recording at least the following details:

* Start day and time
* Duration
* Trigger (whether executed manually or automatically (scheduled))
* Status (error, error-free, ...)