

Security Policy   
Outsourcing

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Outsourcing | |  |
| 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 | Service provider management 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 Principles 4](#_Toc107920366)

[2 Goals 4](#_Toc107920367)

[3 Controls 4](#_Toc107920368)

# Principles

A process for the selection and management of outsourcing providers (including cloud service providers) must be established, supported by documented agreements setting out the security requirements to be met.

# Goals

Ensure that security requirements are met and maintained when a specific environment or service is provided by an outsourcing provider.

# Controls

A documented process must be set up that regulates the selection of outsourcing providers and the transfer of activities to them.

When defining the requirements for outsourcing, SÜDVERS:

* Assess cross-border/multi-country legal and regulatory information risks associated with outsourcing arrangements and the specific business functions that may be outsourced
* Identify requirements (e.g. in relation to privacy, data protection, encryption export and data breach notification)
* Identify particularly critical or sensitive business environments
* consider the classification of the information to be placed in the care of the outsourcing provider
* Evaluate and review the information security practices and standards of potential outsourcing providers
* Consider dependencies between the service or function to be outsourced and other services or business functions
* have defined strategies for exiting the relationship in the event of termination of the agreement.

Before the management of a particular business environment is transferred, the information security management and technical information security controls must be agreed with the outsourcing provider and the approval of the relevant business owners for the transfer must be obtained.

Contracts concluded with outsourcing providers (including cloud service providers) must:

* be reviewed by an independent party (e.g. a legal representative, lawyer or equivalent) from the relevant specialist department
* be approved by the management
* each be agreed and signed by an authorized person representing the respective party
* be kept up to date.

Contracts with outsourcing providers must oblige them to provide all services within their scope:

* comply with all applicable laws relevant to SÜDVERS (including (but not limited to) those relating to data protection, data breaches, data export, encryption export and use, and REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience in the financial sector (DORA))
* adhere to the best practices for
  + Information security management
  + Technical information security
  + Information risk management
  + IT service management
* Compliance with the manufacturer's recommendations
* comply with the information security guidelines of SÜDVERS
* maintain the confidentiality of the information obtained under the outsourcing agreement
* protect the integrity of the information used in the context of the work
* Ensure the availability of information and systems
* Provide information on information security incidents in a timely manner.

The contracts must stipulate that the outsourcing providers are obligated:

* restrict access to the assets of SÜDVERS to authorized employees
* define the manner in which they are permitted to outsource other external parties.
* ensure the quality and accuracy of the work performed
* follow a change management process
* Ensure effective management of incidents and problems in the area of information security
* ensure that SÜDVERS can meet the 72-hour deadline for reporting data breaches to the authorities
* For SÜDVERS in accordance with EU Regulation 2022/2554 to report security incidents subject to mandatory reporting to SÜDVERS within 3 hours or to make the initial report to the competent reporting authorities within 4 hours and to inform SÜDVERS immediately . If the service provider is unable to make this assessment, the 3-hour reporting obligation to SÜDVERS applies
* ensure that SÜDVERS can meet the deadline for reporting DORA-relevant security incidents to the authorities
* Return or destruction of information, software and equipment belonging to SÜDVERS at an agreed time or on request
* take effective precautions for business continuity and crisis management
* ensure that SÜDVERS can meet the forensic requirements and associated deadlines required by applicable laws, law enforcement authorities or other relevant third parties.

The contracts must also state:

* All regulations in accordance with EU Regulation 2022/2554 Art. 30
* the details of the license agreements
* Regulations regarding ownership of intellectual property rights and information
* the right of SÜDVERS to review the activities of the outsourcing provider.