

Security Policy   
Cloud Computing

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Cloud Computing Directive | |  |
| 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 guideline | |
| 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](#_Toc194566001)

[2 Goals 4](#_Toc194566002)

[3 Controls 4](#_Toc194566003)

[3.1 Policy for cloud computing 4](#_Toc194566004)

[3.2 Cloud computing contracts 6](#_Toc194566005)

# Principles

A comprehensive, documented policy for the use of cloud services must be drawn up and communicated to all persons who may purchase or use cloud services.

# Goals

Ensure that all relevant persons (e.g. project managers) at SÜDVERS are aware of the instructions and requirements of the management with regard to the purchase and use of cloud services.

# Controls

## Policy for cloud computing

The information security function should support the business functions (e.g. procurement and legal) in defining standard/contractual requirements for the purchase and use of cloud services.

Cloud service providers must at least meet the following standards (or equivalent) (whether certified or not):

* ISO 27001ff
* ISO 27017
* ISO 27018
* ISO 27701
* ISO 22301
* ISO 20000ff
* ISAE 3402
* 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)
* Where relevant: PCI DSS v4.x

Before purchasing or using cloud services, an information risk assessment must be carried out that takes the following into account

* Type, classification and significance of the information that can be processed in the cloud
* Legal/regulatory risks for SÜDVERS
* Financial risks for SÜDVERS
* Operational risks for SÜDVERS
* Employee-related risks for SÜDVERS
* the impact on data protection

An information risk assessment must be conducted for each cloud initiative to identify the security measures required to protect the information handled in the cloud throughout its lifecycle, including

* Creation of information
* Processing
* Storage
* Transmission
* Destruction

Based on the results of the information risk assessment and the classification of information that can be processed in the cloud, a decision must be made as to whether information:

* must not be stored in the cloud (e.g. if it concerns sensitive personal data or strictly confidential business information, e.g. in connection with mergers and acquisitions)
* must be encrypted during storage and transmission to/from the cloud
* there are restrictions on storage and processing in certain jurisdictions.

A procedure must be introduced to ensure that the use of cloud services (including general cloud services)

* is identified and recorded in a register (or equivalent document)
* is approved by both the business owners and the SÜDVERS IT architecture (or equivalent)
* is supported by a contract
* be checked at regular intervals

SÜDVERS IT must provide technical means to protect the information stored in the cloud, including at least the following:

* Development of a technical security infrastructure that is compatible with the cloud provider's architecture and infrastructure
* Maintaining the compatibility of the client systems for each cloud service with SÜDVERS IT standards (e.g. by monitoring the browser version and plug-in requirements)
* Use of secure communication technologies between SÜDVERS and the cloud services used.

SÜDVERS IT must help ensure the availability of access to information stored in the cloud by

* Investments are made in robust, reliable Internet connections
* several connection methods can be set up
* the required network bandwidth is available between the SÜDVERS network and the cloud service provider
* Connections to/from SÜDVERS legacy systems are ensured

## Cloud computing contracts

Any use of cloud computing services must be underpinned by a contract (including terms and conditions or equivalent) that contains all the clauses that apply to standard contracts with external suppliers and that contains specific provisions for the use of cloud services.

The contracts must:

* To be checked by SÜDVERS specialist department, legal department, IT and information security before conclusion
* be approved and signed by an authorized person representing each party
* are subject to the standard procurement processes of SÜDVERS
* be kept in a safe place so that they can be verified in the event of a dispute.

The contracts must oblige the cloud service provider to protect SÜDVERS' information by:

* Provision of a secure authentication service that meets the requirements of SÜDVERS for identity and access management (IAM) (e.g. including all requirements for federated identity and access management)
* Restricting access to authorized users (e.g. through access control lists, whitelists or blacklists)
* Restriction of access to cloud services if the connections come from outside the SÜDVERS company firewall
* Management of access controls of the cloud service to meet the requirements of SÜDVERS
* Implementation of suitable solutions for monitoring and protection against malware
* Provide a method for the secure destruction of SÜDVERS information stored in the cloud once it is no longer required (e.g. in accordance with the SÜDVERS document retention policy or equivalent).

The contracts must require the cloud provider to share security-related information about unusual or malicious activity based on SÜDVERS' requirements, including details of:

* User/system activities
* unauthorized changes to critical permanent (or static) information, such as customer master files, manufacturing data, price tables and exchange rates
* Event logs, alerts and reports generated by intrusion detection systems (IDS) and data loss protection (DLP) systems
* Results of network traffic monitoring to provide early warning of potential attacks (including malicious network traffic).

Cloud service contracts must require the provider to comply with the requirements to protect SÜDVERS' sensitive data (including personally identifiable information (PII)) by:

* Processing and storage at authorized locations or within a specific jurisdiction
* solutions based on recognized industry standards for IT architecture and IT infrastructure.

Cloud service contracts must oblige the provider to fulfill the availability requirements of SÜDVERS by:

* Provision of dedicated support (e.g. identified support personnel and method of contacting them directly) in the event of a security incident in the cloud
* Ensuring that SÜDVERS' security requirements are met if cloud services are subcontracted to an external provider or subcontracting of cloud services is not permitted
* Supporting SÜDVERS in the event of legal action initiated by or against SÜDVERS concerning SÜDVERS' information (e.g. e-discovery requests or forensic investigations)
* provides an escrow system (e.g. for information, proprietary technologies, application source code and cryptographic keys) using a trusted external provider.

The contracts must require cloud service providers to inform SÜDVERS in advance of any changes to the way in which the service is provided, in particular in the event of

* Relocation of the technical IT infrastructure to another geographical region or another jurisdiction
* Processing or storing information in a new geographical area or jurisdiction