

Governance Model

Information Security

|  |  |
| --- | --- |
|  |  |
| Governance model |  |
| Number | [Number] |
| Issued on | 21.06.2022 |
| Through | Chief Information Security Officer |
| Entry into force | 21.06.2022 |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH |
| Topic | Information security |
| Responsible function | Information security |
| Responsible person | Dirk Franken |
| Overriding regulation | [Parent regulation] |
| 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 Governance of information security 4](#_Toc194573075)

[2 Roles and responsibilities 5](#_Toc194573076)

[2.1 Data Protection, Information Security and IT Standards Committee 6](#_Toc194573077)

[2.2 Management 7](#_Toc194573078)

[2.3 Information Security Officer 8](#_Toc194573079)

[2.4 IT Security and IT Architecture Committee 8](#_Toc194573080)

[2.5 Data Protection Officer 9](#_Toc194573081)

[2.6 Head of IT 10](#_Toc194573082)

[2.7 IT Business Continuity Manager 10](#_Toc194573083)

[2.8 Legal department 11](#_Toc194573084)

[2.9 Personnel department 11](#_Toc194573085)

[2.10 System owner 11](#_Toc194573086)

[2.11 Information owner 11](#_Toc194573087)

[2.12 Project manager 12](#_Toc194573088)

[2.13 IT/Network/Security Administrator 13](#_Toc194573089)

[2.14 Employees in the specialist departments and staff units 13](#_Toc194573090)

# Governance of information security

The SÜDVERS Information Security Governance Model described in this document applies to all employees of the SÜDVERS Group who store, process or transmit information, regardless of the nature of their employment. In addition, by defining a governance model, it establishes the organizational basis for the secure processing, transmission and storage of information with stakeholders, partners and suppliers. It concerns the management of all information, regardless of its form and the associated IT systems and security systems within SÜDVERS, as well as information that is stored, processed or transmitted outside of SÜDVERS insofar as it is subject to the legal or contractual control of SÜDVERS.

In order to establish appropriate governance for information security in the company, the SÜDVERS will

* act as the governing body of SÜDVERS for information security and, as part of its associated management role, define, manage, monitor and communicate the framework conditions for the governance of information security.
* Ensure that information security is treated as a critical business issue.
* Establish at least the following corporate functions:
  + a data protection, information security and IT standards committee directly assigned to the management. In addition, a member is appointed at management level who assumes overall responsibility for the information security governance model and chairs and steers the Data Protection, Information Security and IT Standards Committee
  + The function of an information security officer as the person responsible for all aspects of information security and information risk management
  + The function of a data protection officer as the person responsible for all aspects of data protection
* ensure that the internal information security policy is supported by an information security strategy
* monitor and review the overall information security objectives of SÜDVERS and the associated risk appetite at least every six months
* demonstrate its commitment to information security by formally approving or enacting the following documents:
  + Overall concept for information security governance (see figure below)
  + Information security strategy
  + risk management strategy
  + Internal rules and regulations for information security
  + Results of the periodic SÜDVERS information security assessments and information risk assessments

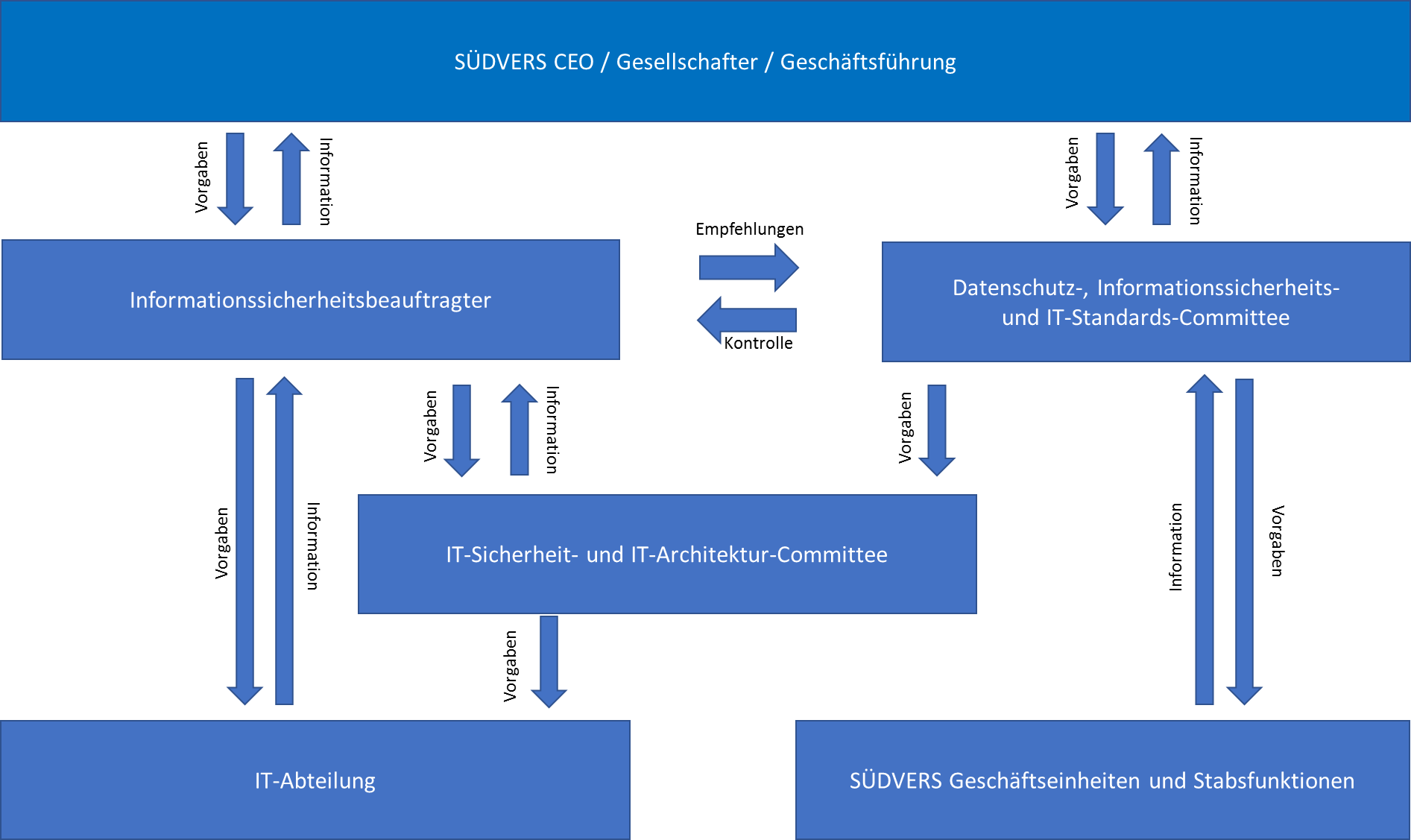
Taking into account the fact that a 100% information security level cannot realistically be achieved for both technical and organizational reasons - and would also not be economically justifiable - SÜDVERS strives for an acceptable level of information security based on international standards (such as ISO/IEC 27000ff), regulatory requirements (such as REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL) and industry-recognized best practices. The specific measures resulting from this approach must be aligned with SÜDVERS' business and culture as well as being effective, efficient, appropriate ("fit for purpose"), consistent and cost-conscious ("fit for resources").

# Roles and responsibilities

Organizationally, the governance model for information security is primarily made up of three roles:

* Data Protection, Information Security and IT Standards Committee, as the primary steering and control body for information security
* Information Security Officer, responsible for all aspects of information security and information risk management
* IT Security and IT Architecture Committee, for the coordination of IT technical and operational aspects of information security

Schematically, this is as follows:



## Data Protection, Information Security and IT Standards Committee

As part of its role in the governance of information security, the Data Protection, Information Security and IT Standards Committee supports the Information Security Officer in defining the overall approach to information security at SÜDVERS by performing the following tasks:

* Formal approval of a business-oriented approach
* Review of the overall strategy for information security and information risk management before approval by the information security officer
* Reviewing which legal requirements exist for SÜDVERS with regard to information security and information risk management, communicating these requirements to the relevant departments and regularly reviewing compliance
* Promoting the continuous improvement of information security at SÜDVERS
* Emphasizing the importance of information security for SÜDVERS
* Integration of information security and information risk management into SÜDVERS' business planning processes
* Integration of information security into the procurement processes of SÜDVERS
* Requesting or providing adequate resources for information security and to meet the requirements for digital operational resilience
* Initiation of independent reviews by the information security organization if:
  + laws and regulations affecting the organization change;
  + significant incidents occur;
  + SÜDVERS opens a new company or acquires an existing company;
  + SÜDVERS significantly changes information security measures and procedures

Furthermore, the Data Protection, Information Security and IT Standards Committee ensures the ongoing effectiveness and efficiency of information security precautions by performing the following tasks:

* Discussion and approval of important decisions that affect the state of information security at SÜDVERS
* Discussing the overall status of information security and initiating corrective measures if necessary
* Promoting timely decision-making in relation to the processing of information risks by monitoring the SÜDVERS risk profile
* Approval of conceptual changes to the information security framework
* Reporting to the responsible corporate bodies
* Establish reporting channels that allow him to be properly informed of the following:
  + agreements concluded with third-party IT service providers on the use of IT services,
  + all relevant planned material changes in relation to third-party IT service providers,
  + the potential impact of such changes on the critical or important functions covered by such agreements, including a summary of the risk analysis to assess the impact of such changes and, as a minimum, of serious IT-related incidents and their impact, as well as countermeasures, recovery and corrective actions

The Data Protection, Information Security and IT Standards Committee

* coordinates information security and information risk management activities at SÜDVERS
* is chaired by the member of the Executive Board appointed for this purpose
* has at least the following members
  + the information security officer
  + the data protection officer
  + the Head of IT
  + the head of the legal department
* meets at least six times a year (participation of permanent members is mandatory) and documents the measures agreed at these meetings
* the Chatham House Rules apply to the meetings of the Committee
* The Committee can make decisions either unanimously by the permanent members or with a 2/3 majority and the approval of the senior management member

## Management

The management is responsible for ensuring that employees implement information security in accordance with the established information security policy and the organization's topic-specific guidelines and procedures.

The responsibilities of the management therefore include that the employees:

* be informed of their roles and responsibilities in information security before being given access to the organization's information and other related assets;
* receives policies that outline the expectations of his or her role in information security within the organization;
* has the task of complying with the organization's information security policy and topic-specific guidelines;
* achieved an information security awareness that corresponds to his roles and responsibilities within SÜDVERS;
* Compliance with the terms and conditions of employment, contract or agreement, including the SÜDVERS Information Security Policy and appropriate working practices;
* has appropriate skills and qualifications in the field of information security through continuous professional development
* as far as practicable, can report violations of the information security policy, topic-specific guidelines or procedures for information security via a confidential channel ("whistleblowing").
* has adequate resources and project planning time for the implementation of security-relevant processes and measures in the organization.

## Information Security Officer

The Information Security Officer was appointed at management level and has overall responsibility for information security and information risk management at SÜDVERS as well as responsibility for the direction of this area.

As part of their role, the Information Security Officer will implement SÜDVERS' overall approach to information security by performing the following tasks:

* Development and maintenance of a strategy that supports the chosen governance model
* Development and maintenance of a set of rules for information security
* Development and maintenance of a set of rules for information risk management
* Management of information security risks
* Carrying out information risk assessments
* Protection of sensitive information from disclosure to unauthorized persons
* Assume responsibility for the development and maintenance of an information security architecture that provides a framework for the application of standard security controls at SÜDVERS
* Ensuring that new or additional IT systems and IT services are developed and/or implemented securely
* Carrying out security checks of SÜDVERS service providers
* Performance of security audits of SÜDVERS by customers or institutions

## IT Security and IT Architecture Committee

In addition to the Data Protection, Information Security and IT Standards Committee at Group level, SÜDVERS has set up a combined IT Architecture and Security Committee for technical aspects of IT security. The combined committee is managed jointly by the Information Security Officer (for security-related aspects) and the Head of IT (for architecture-related aspects).

As part of its information security-related tasks, the combined body will

* coordinate the technical-operational IT security activities at SÜDVERS,
* ensure that IT security is viewed as an integral part of the IT architecture,
* ensure that information security is treated as an essential element of all IT-related aspects and activities
* monitor the internal IT security objectives and review them at least every six months
* meet at least quarterly and document the measures agreed at these meetings

As part of its security responsibilities, the combined body should ensure the ongoing effectiveness and efficiency of IT security arrangements by

* discusses and approves important decisions concerning the technical-operational IT security status of SÜDVERS
* discusses the overall status of technical-operational IT security and, if necessary, initiates corrective measures
* Ensure that the information security framework and the technical security architecture framework are aligned
* discuss conceptual changes to the technical IT security aspects of the information security framework

The members of the combined IT Architecture and IT Security Committee include:

* the information security officer
* the Head of IT
* the person responsible for the network infrastructure
* the person responsible for the server infrastructure
* the person responsible for the critical business applications

The combined IT architecture and IT security committee meets at least four times a year and documents the measures agreed at these meetings

## Data Protection Officer

The Data Protection Officer is responsible for data protection within SÜDVERS. The detailed competencies and responsibilities as well as the reporting lines are defined in the applicable data protection laws.

With regard to information security aspects, the data protection officer is responsible for the following:

* Contact person for the Information Security Officer for all data protection issues
* Ensuring that data protection requirements are fully covered by the information security guidelines

## Head of IT

With regard to information security aspects, the Head of IT is responsible for the following:

* Allocate sufficient resources and manage staff to ensure that IT systems are designed, built and operated in a secure, reliable and manageable way that meets SÜDVERS' business objectives
* Ensuring compliance with the information security policy, strategies and guidelines with regard to all aspects in his/her area of responsibility
* Review and approval of important purchases and contracts for a large number of IT projects
* Ensuring that all SÜDVERS employees carry out their daily activities with the IT systems in a manner that is compliant with the SÜDVERS information security guidelines
* Designing new IT architectures, strategies and processes that support SÜDVERS' business objectives
* Documentation and management of the IT architecture
* Definition, implementation and monitoring of compliance with IT guidelines for the implementation of technical information security guidelines
* Ensuring that the information security aspects of information risk management are taken into account in IT projects
* Implementation of at least annual BCM tests and emergency tests for all defined BCM and emergency scenarios, including implementation of lessons learned activities and adaptation of processes where necessary

## IT Business Continuity Manager

With regard to information security aspects, the IT Business Continuity Manager (among others) is responsible for the following:

* Coordinate business and information security contingency planning so that integrated contingency planning covers all areas critical to SÜDVERS' business
* Research and keep abreast of any major threats that could impact SÜDVERS' business activities, including mergers and acquisitions, environmental threats, changes in economic conditions, ...
* Carrying out regular assessments of the impact on the business in accordance with the risk assessment methodology defined in this manual
* Training users in the proper use of emergency planning documents relevant to business resources
* Existence of IT-BCM and emergency plans for the IT-supported business processes of SÜDVERS as well as the respective IT infrastructure and the at least annual execution of the tests of the plans and scenarios
* Support in creating practical and integrated SÜDVERS-wide contingency plans that combine information security contingency plans with business contingency plans

## Legal department

Continuous monitoring of all laws and regulations applicable to SÜDVERS and informing SÜDVERS' internal departments about changes / innovations.

With regard to information security aspects, the Legal department is responsible for providing guidance on regulatory and legal aspects of information security, data protection and REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of December 14, 2022 on digital operational resilience in the financial sector (DORA) upon request.

## Personnel department

With regard to information security aspects, the HR department is responsible for the following tasks

* Inclusion of information security aspects in the employee life cycle
* provide sufficient and appropriate information security training for employees
* Ensuring that SÜDVERS employees have security certificates and have passed the required personal security checks
* Responsibility for the physical access control process and for the implementation of related HR activities

## System owner

The system owners have overall responsibility for the systems in their area of responsibility. As part of their role, they are responsible for full compliance with the information security guidelines in relation to all applicable aspects. In particular, the system owners are responsible for assessing the business impact and risks to their systems, classifying them and instructing the IT/network/security administrators in their security-related tasks.

## Information owner

Information owners are designated for the protection of information. The information owners are responsible for the classification, use and application of suitable protective measures for the sensitive data assigned to them. They assign and review access rights to information or applications while maintaining an appropriate scope.

## Project manager

Project managers are responsible for compliance with information security guidelines and information risk management aspects of their projects.

A person in this role is responsible, among other things, for ensuring that:

* information security risks are assessed and addressed at an early stage and regularly as part of the project risks throughout the project life cycle;
* Information security requirements [e.g. e.g. application security requirements, intellectual property rights compliance requirements, etc.] are addressed in the early phases of projects;
* the information security risks associated with the implementation of projects, such as the security of internal and external communication aspects, are considered and addressed throughout the entire project life cycle;
* progress in addressing information security risks is reviewed and the effectiveness of the treatment is assessed and audited.

When determining the requirements, the following points must be taken into account in addition to others:

* what information is involved (information determination), what information security requirements are associated with it (classification) and what potential negative business effects may result from a lack of adequate security;
* the necessary protection requirements for information and other related assets, in particular with regard to confidentiality, integrity and availability;
* the required level of trust or trustworthiness in relation to the identity specified by the entities to derive the authentication requirements;
* Access allocation and authorization processes for customers and other potential business users as well as for privileged or technical users such as relevant project members, potential operational staff or external suppliers;
* informing users about their duties and responsibilities;
* the requirements derived from the business processes, such as the logging and monitoring of transactions and requirements relating to non-repudiation;
* the requirements imposed by other information security measures (e.g. interfaces to logging and monitoring systems or data loss detection systems);
* compliance with the legal, statutory, regulatory and contractual framework conditions;
* Level of confidence or trustworthiness required for third parties to comply with SÜDVERS information security policy and topic-specific guidelines, including the relevant security sections in any agreements or contracts.

## IT/Network/Security Administrator

IT/Network/Security Administrators are responsible for the definition, implementation and technical maintenance of devices and technologies that make up SÜDVERS' IT environment.

A person in this role is responsible for, among other things:

* Definition and implementation of technical security measures at SÜDVERS
* Participation in the risk management process in the role of a technical expert
* Maintenance of infrastructure and resources
* Monitoring of access rights to SÜDVERS resources
* Monitoring and maintenance of SÜDVERS' infrastructure and resources
* Management of availability and events
* Responding to threats and security incidents in SÜDVERS
* Support and implementation of components within the SÜDVERS IT BCM are
* Raising user awareness in technological areas

## Employees in the specialist departments and staff units

With regard to information security aspects, a user is any employee, contractor or third-party provider of SÜDVERS who is authorized to access the information systems and/or information of SÜDVERS.

A user is responsible for the following aspects of information security:

* Compliance with information security guidelines
* Reporting actual or suspected vulnerabilities that affect the confidentiality, integrity or availability of SÜDVERS information to the IT helpdesk
* Reporting actual or suspected breaches of the confidentiality, integrity or availability of SÜDVERS information to the IT helpdesk