

Architectural principles

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Architecture principles | |  |
| Number | [Number] | |
| Issued on | 19.06.2023 | |
| Through | Chief Information Security Officer | |
| Entry into force | 01.10.2023 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Topic | Information technology & data protection | |
| Responsible function | Information security | |
| Responsible person | Dirk Franken | |
| Overriding regulation | Information security policy | |
| Replaces | n/a | |
| Applicable documents |  | |
| Validity | Until further notice | |
| Last review | 14.07.2025 | |
| Next review | 07.01.2026 | |
| Publication | SÜDVERS Intranet | |
| Classification | Internal | |
| Archive | Document management system | |
| Organizational system | [Organizational system] | |
| Languages |  | |
| Formats |  | |
| Remarks |  | |

Security governance

* Establish, maintain and monitor an information security governance framework that enables SÜDVERS to provide clear direction and demonstrate commitment to information security and risk management.
* Supporting the information security governance framework by developing an information security strategy and implementing measures to ensure compliance with the information security strategy and the information security policy that are aligned with SÜDVERS' strategic objectives

Assessment of information risks

* Conduct regular information risk assessments for target environments (e.g. critical business environments, processes and applications, including supporting systems/networks) in a rigorous, consistent manner and using a systematic, structured methodology
* Apply an information risk assessment methodology that includes key activities such as scoping, business impact assessment, threat profiling, vulnerability assessment, risk assessment and risk treatment

Information security management

* Establish a specialized information security function with appropriate authority and resources to carry out information security-related projects, promote information security at SÜDVERS and consider the impact of relevant laws, regulations and contracts
* Developing a comprehensive, approved information security framework and communicating it to all individuals with access to SÜDVERS information and systems

Personnel management

* Embedding information security at every stage of the employment lifecycle, which includes
  + the assignment of ownership of information (including responsibility for its protection) to appropriately qualified persons, and
  + Obtaining confirmation that these persons understand and accept this
* Maintain a comprehensive, ongoing security awareness program to promote and embed expected security behaviors among all individuals who have access to SÜDVERS' information and systems.

Information management

* Introduction of a classification scheme for all types of information (e.g. physical, electronic and oral information), supported by guidelines for handling information to protect it from corruption, loss and unauthorized disclosure
* Assigning responsibility for managing data protection at SÜDVERS to a Data Protection Officer (or equivalent), which includes carrying out data protection assessments and protecting personal data (e.g. information that can be used to identify an individual).

Management of physical assets

* Protecting physical assets, including systems and network equipment, office equipment (e.g. network printers and multifunction devices) and specialized equipment (e.g. industrial control systems) throughout their lifecycle, taking into account information security requirements at acquisition (e.g. purchase or lease), maintenance and disposal
* Protecting mobile devices (including laptops, tablets and smartphones) and the information they process from unauthorized disclosure, loss and theft:
  + Configure security settings
  + Restriction of access
  + Installation of security software and
  + Central management of the devices

System development

* Introduction of a structured system development methodology that:
  + applies to all types of business applications (including associated systems and networks);
  + is supported by specialized, separate development environments and
  + includes a quality assurance process
* Develop business applications in accordance with an approved system development lifecycle that includes the application of best industry practices and the incorporation of information security at every stage of the lifecycle:
  + Gathering the requirements; design
  + Acquisition (including purchase and leasing)
  + Creation; testing; implementation
  + and decommissioning

Management of business applications

* Integration of information security controls into business applications (including specific controls for web browser-based applications) to protect the confidentiality and integrity of information as it is input to, processed by, and output from those applications.

System access

* Restrict access to business applications, mobile devices, systems and networks to authorized individuals for specific business purposes by requiring that they:
  + Access privileges are granted according to their role
  + authenticated with the help of strong access control mechanisms
  + must go through a rigorous login process before they are granted authorized access rights
  + Access rights are reviewed at least annually, and at least every six months for IT systems of medium criticality
* Protecting business applications that provide access to customers by conducting risk assessments to determine information security requirements and implementing security measures supported by agreed and approved contracts

System administration

* Develop systems to handle current and forecasted workloads and configure them consistently and accurately to protect them and the information they process and store from:
  + Malfunction
  + Cyber attack
  + unauthorized disclosure
  + Falsification
  + and loss
* Manage the security of systems by creating backups of critical information and software, applying a rigorous change management process and monitoring performance against agreed targets.

Networks and communication

* Design of physical, wireless and voice networks to:
  + are reliable and resistant
  + prevent unauthorized access
  + Encrypt connections
  + and detect suspicious data traffic
* Configure network devices (including routers, firewalls and wireless access points) to function as required and prevent unauthorized or incorrect updates.
* Protection of electronic communication systems (e.g. e-mail, instant messaging, VoIP, telephony and web conferencing facilities) through
  + Definition of guidelines for their use
  + the configuration of security settings
  + and hardening of the supporting technical infrastructure.

Service provider management

* Identifying and managing information risks at each stage of relationships with external suppliers (including: suppliers of hardware and software throughout the supply chain; outsourcing specialists; and cloud service providers),
* by enshrining information security requirements in formal contracts and obtaining assurances that they will be met
* Establish and enforce a comprehensive cloud security policy that specifies the need to include specific information security requirements in cloud-specific contracts and that is communicated to all individuals who purchase or use cloud services.
* Consideration of the specific requirements of EU Regulation 2022/2554 (DORA)

Management of technical security

* Building a solid technical security infrastructure using security architecture principles and integrating technical security solutions that include
  + Protection against malware
  + Identity and access management
  + Use of intrusion detection and prevention systems
  + Use of data loss prevention systems
  + Protection against loss of information
* Use of recognized cryptographic solutions (such as encryption, public key infrastructure and digital signatures) in a consistent manner at SÜDVERS to help:
  + protect the confidentiality of information
  + determine whether critical information has been changed
  + ensure strong authentication
  + and to support non-repudiation

Threat and incident management

* Management of threats and vulnerabilities related to business applications, systems and networks:
  + Scanning for technical vulnerabilities
  + Maintaining current patch statuses
  + Continuous monitoring of security events
  + Responding to information about threats; and
  + Protecting information from targeted cyberattacks
* Establish a comprehensive and approved information security incident management framework supported by an information security incident identification, response, recovery and post incident review process and integrate it into the overall incident handling process.
* Consideration of the specific requirements of EU Regulation 2022/2554 (DORA)

Management of the local environment (buildings, data centers)

* Protection of critical facilities and services:
  + targeted cyber attacks
  + unauthorized physical access
  + Accidental damage
  + Power failure
  + fire; and
  + other environmental or natural disasters

IT business continuity planning (BCM)

* Development of a SÜDVERS IT business continuity strategy and an IT business continuity program supported by a resilient technical IT infrastructure and effective crisis management.
* Development, maintenance and regular testing (at least annually per system environment) of IT business continuity plans and agreements (sometimes also referred to as disaster recovery plans) for critical business processes and applications at SÜDVERS.
* Consideration of the specific requirements of EU Regulation 2022/2554 (DORA)

Safety monitoring and improvement

* Conduct thorough, independent and regular audits of the security status of target environments (critical business environments, processes, applications and supporting systems/networks).
* Regular monitoring of information risks, compliance with security-related elements of legal, regulatory and contractual requirements and the overall state of information security at SÜDVERS and reporting the results to specific target groups, such as the Management Board.