

Information Security Strategy

Information Security

|  |  |  |
| --- | --- | --- |
|  | |  |
| Information security strategy | |  |
| 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 | | Information security 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 | |  |

Because we as SÜDVERS depend on the use of information and technology, managing the associated information security requirements is important. If important information is disclosed to the wrong people, is unavailable or unreliable, this could have a direct or indirect operational and/or financial impact on our company or our customers. If information is disclosed to unauthorized persons, this could lead to damage to our reputation, civil or possibly even criminal liability in addition to the internal financial impact.

The primary objectives of the information security strategy are therefore:

* Creating a framework for information security
  + Creating a framework for information security and information security management from an IT and business management perspective that is risk-oriented and aligned with both SÜDVERS' culture and industry best practices
* Ensuring an appropriate overall level of maturity for information security by
  + Management of information security according to best practice as defined in ISO/IEC 27001
  + Implementation of information security controls that are generally regarded as best practice (e.g. in ISO/IEC 27002)
  + Ensure that information security is embedded in the IT project management lifecycle
* Control the costs associated with information security by
  + Application of existing, proven and tested methods for information security
  + Standardization and traceability of the methods used
  + Implementation of a continuous improvement program
  + Support other strategic information security or information risk management initiatives by providing an overall information security framework
* Ensuring compliance with legal or contractual requirements by:
  + Supporting the GDPR and other country-specific data protection regulations by providing the basis for the information security elements of these standards
  + Supporting 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) by providing the basis for the information security elements of this regulation
  + Providing the basis for the information security elements to ensure that information covered by the Data Protection Act is adequately protected
  + Supporting the requirements of ISO/IEC 27001/2 by providing the basis for the information security elements of this standard

To ensure that we approach these initiatives in the most appropriate and secure manner, we aim to base them on the generally accepted best practices for information risk management, which are consistent with SÜDVERS' information security framework. In addition to complying with corporate governance frameworks, we will also comply with the requirements or recommendations set out in auditing standards or data protection laws.

By aligning ourselves with ISO standards and information security management best practice standards and following information security best practice, we can demonstrate that we are doing the right things and that we are doing them in the right way.