

Information Risk Management Strategy

Information Security

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | |
| Information risk management 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 risk management strategy are therefore:

* Control of information risks at the level of general risk management
  + Creation and management of information risk assessments from the perspective of IT and overall company management
  + Ensuring that information risks are recorded in the comprehensive corporate risk register
* Ensuring an appropriate governance structure for the management of information risks by
  + Management of information risks according to recognized best practices
  + Implementation of information risk management controls that are recognized as best practice
  + Ensuring that information risk management is integrated into IT project management
* Controlling the costs associated with information risks by
  + Application of proven and tested methods of information risk management
  + Standardization and traceability of the methods used
  + Implementation of a continuous improvement program
* Ensuring compliance with legal or contractual requirements by
  + Providing the basis for the elements of information risk management to ensure that information covered by data protection law is adequately protected
  + Supporting the requirements of "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 risk management elements of these standards
  + Support the requirements of ISO/IEC 27001, ISO/IEC 27005 and ISO 27036 by providing the basis for the information risk management elements of this standard
  + Support of customer requirements regarding information security management in the context of the activities of SÜDVERS as a service provider, which provides IT systems for customers, processes, stores or transports customer data on SÜDVERS systems.
* Supporting other strategic information security or information risk management initiatives by providing a general framework for information risk management that forms the basis for the risk management elements of certification activities

To ensure that we approach these initiatives in the most appropriate and secure manner, we strive to base them on generally accepted best practices for information risk management that are consistent with SÜDVERS' information security framework.

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

By applying industry-recognized best practice methods and approaches, we ensure compliance with risk management requirements in the area of information security as set out in ISO/IEC 27000ff, ITIL, ISO/IEC 20000, ISO/IEC 22301 and other industry-specific requirements (e.g. 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)).

In addition to complying with the corporate governance framework, we will also comply with the requirements or recommendations set out in auditing standards or data protection laws.