

Information security policy

Information Security

|  |  |
| --- | --- |
|  |  |
| Information security policy |  |
| 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 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 |  |

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.

In this context, and taking into account the fact that a 100% information security level cannot realistically be achieved for technical and organizational reasons - and would also not be economically viable - **SÜDVERS strives for an acceptable level of information security based on international standards** (such as ISO/IEC 27000ff.standards (such as ISO/IEC 27000ff)**, industry-wide recognized best practices and** fully complies **with legal** requirements (e.g. GDPR or 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)).

To ensure this, SÜDVERS will establish an information security framework based on the following elements:

* SÜDVERS Industry and culture
* Risk awareness and
* Compliance with international standards for both information security management and technical, operational information security

The specific information security measures resulting from this approach must be aligned with SÜDVERS' industry and culture as well as being effective, efficient, appropriate ("fit for purpose"), consistent and cost-conscious ("fit for resources"). Particular attention is paid to the smooth and uninterrupted operation of services for our customers and to the protection of SÜDVERS' reputation.

The SÜDVERS framework for information security corresponds to the structure of ISO/IEC 27002 and deals with the building blocks of information security listed below:

* Organizational measures,
* Personal measures,
* Physical measures, and
* Technological measures

The associated topic-specific SÜDVERS information security guidelines are published in the SÜDVERS document archive d3 and via other suitable media.