

Security Policy   
Compliance

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Security Policy Compliance | |  |
| Number | [Number] | |
| Issued on | 04.07.2022 | |
| Through | Chief Information Security Officer | |
| Entry into force | 04.07.2022 | |
| Scope of application | SÜDVERS Holding GmbH & Co. KG and its majority-owned subsidiaries, as well as SÜDVERS International GmbH | |
| Topic | Compliance | |
| 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 |  | |

Table of contents

[1 Principles 4](#_Toc175311921)

[2 Goals 4](#_Toc175311922)

[3 Controls 4](#_Toc175311923)

# Principles

A process must be defined and implemented to determine and interpret the impact of laws and regulations directly or indirectly applicable to SÜDVERS on information security.

# Goals

Ensuring compliance with laws and regulations relating to information security.

# Controls

Legal and regulatory requirements relating to information security must be known to at least the following bodies and roles:

* the management
* the data protection officer
* the information security officer
* the Head of IT
* Representatives of other security-related functions (e.g. legal department, internal audit, human resources).

A process must be established that ensures compliance with the relevant legal and regulatory requirements relating to information security at SÜDVERS and covers at least the following legal areas

* Information security-specific legislation (e.g. cybercrime, encryption export, data breach notification and e-discovery)
* EU Regulation 2022/2554 (DORA)
* general legislation that has an impact on security (e.g. data protection, investigative powers, intellectual property and human rights)

A process must be established to ensure an appropriate flow of information regarding information security between SÜDVERS and the relevant judicial, regulatory and supervisory authorities.

The compliance process must enable decision-makers to do this:

* Identify laws and regulations that impact information security
* interpret the impact of the discovered laws and regulations on information security
* Recognize potential non-compliance with laws/regulations
* Address areas of potential non-compliance with laws/regulations.

The compliance process must be documented, signed off by the management and kept up to date.

Compliance with laws and regulations relating to information security must be checked:

* carried out regularly and when new legal or regulatory requirements come into force
* Involve representatives from the most important areas of SÜDVERS (e.g. management, the legal department, IT and the information security function)
* lead to an update of the information security guidelines and the associated IT standards to take account of all necessary changes.