

Security Policy   
Reporting of security incidents

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Reporting of security incidents | |  |
| Number | [Number] | |
| Issued on | 01.03.2025 | |
| Through | Chief Information Security Officer | |
| Entry into force | 01.07.2025 | |
| 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 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 |  | |

Table of contents

[1 Principles 4](#_Toc107923369)

[2 Goals 4](#_Toc107923370)

[3 Controls 4](#_Toc107923371)

# Principles

All employees and users must be made aware of their responsibility to report information security incidents as quickly as possible to prevent or minimize the impact of information security incidents.

# Goals

Support the timely, consistent and effective reporting of information security incidents that can be identified by employees.

# Controls

Employees must report information security events (incidents, breaches and vulnerabilities) to the designated central IT contact point; this can be done in person or via the ITSM portal.

Situations to consider when reporting information security incidents include, but are not limited to:

* ineffective information security measures;
* Violations of the expected confidentiality, integrity or availability of information;
* human error;
* Non-compliance with the information security policy, topic-specific guidelines or applicable standards;
* Violations of physical security measures;
* System changes that have not gone through the change management process;
* Malfunctions or other abnormal system behavior of software or hardware;
* Access violations;
* Weak points;
* suspected infection by malware.

Employees and users are strongly discouraged from attempting to independently detect suspected information security vulnerabilities rather than leaving this to the trained specialists within our IT department. Testing vulnerabilities may be interpreted as potential misuse of the system and may also result in damage to the information system or service and damage or render unrecognizable digital evidence. Ultimately, this can result in legal liability for the employee carrying out the work.