

Security Policy   
Incident Management

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Incident Management | |  |
| 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 Principle 4](#_Toc188346706)

[2 Objective 4](#_Toc188346707)

[3 Controls 4](#_Toc188346708)

[3.1 Basics 4](#_Toc188346709)

[3.2 Contact with special interest groups 5](#_Toc188346710)

[3.3 Information on the threat situation 6](#_Toc188346711)

# Principle

A framework for the management/handling of information security incidents based on internationally recognized service management standards must be created, which includes the regulations regarding persons, information and tools required for the management of information security incidents in the organization.

# Objective

Providing the necessary resources to resolve information security incidents quickly and effectively.

# Controls

## Basics

SÜDVERS designates NIST SP800-61 as the applicable framework for information security incident management.

The defined framework for information security incident management must be supported by documented standards/procedures that:

* Define the roles and responsibilities of the team for managing and reporting security incidents
* Determine the types of information needed to support information security incident management (e.g., security event log data, network configuration diagrams, and information classification details)
* Specify the tools required to support information security incident management (e.g. checklists, e-discovery software, log analyzers, incident tracking software and forensic analysis software, SIEM, SOAR ...)
* require details of information security incidents to be collected and reviewed.

An information security incident management team must be set up that

* has defined roles and responsibilities
* has sufficient skills/experience in dealing with information security incidents
* has the authority to make critical business decisions and escalate incidents

The information required for handling information security incidents must be easily accessible and include at least the following

* Contact details of relevant parties (e.g. head of the specialist department, operational specialists, technical experts and external suppliers)
* Security-related event logs (e.g. those generated by applications, systems, network devices and security products)
* Details of affected business environments (e.g. processes, workflows and applications)
* Technical details (e.g. network diagrams, system configurations and external network connections)
* Information about threats and the results of threat analyses.

Details of information security incidents (e.g. type and category of incident, information affected and events leading to an incident) must be recorded and maintained on an ongoing basis, using a consistent approach (e.g. using an agreed taxonomy).

Information on security incidents must be collected and regularly reviewed in order to:

* comply with the regulatory reporting requirements (e.g. with regard to GDPR or DORA)
* Identify patterns and trends in information security incidents
* Understand the costs and impacts associated with the incidents
* assess the operational impact
* determine the effectiveness of controls (e.g. which controls are better suited to preventing, detecting and delaying incidents or minimizing the impact of incidents on the company)
* enable a comparison of internal and external information on incidents
* improve future information risk assessments and security audits.

## Contact with special interest groups

Membership of interest groups or forums should be considered in order to:

* improve knowledge of best practice and the state of the art and keep up to date with relevant safety information;
* ensure that the understanding of the information security environment is up to date;
* receive timely warnings, tips and patches to protect against attacks and vulnerabilities;
* gain access to expert advice on information security;
* Exchange information about new technologies, products, services, threats or vulnerabilities;
* provide appropriate liaison points when dealing with information security incidents

## Information on the threat situation

Information about existing or emerging threats can be divided into three layers, all of which should be taken into account:

* Strategic threat analysis: exchange of high-level information on the changing threat landscape;
* Tactical threat data: Information about the attackers' methods, tools and technologies;
* operational threat data: Details of specific attacks, including technical indicators

and should be collected and evaluated in order to:

* to facilitate informed steps to prevent the threats from harming the organization;
* reduce the impact of such threats.

The use of external specialized service providers or government agencies to obtain threat intelligence is recommended.