

Security Policy   
Web filtering

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Web filtering | |  |
| 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 Content

[1 Principles 4](#_Toc107923369)

[2 Goals 4](#_Toc107923370)

[3 Controls 4](#_Toc107923371)

# Principles

To avoid the risk of your employees accessing websites that contain illegal information, are used to upload data or are known to contain viruses or phishing material, access to external websites must be managed centrally.

# Goals

Protection of systems against the intrusion of malware and prevention of access to unauthorized web resources.

# Controls

SÜDVERS must determine the types of websites to which employees should and should not have access. In general, access to the following types of websites must be technically blocked for reasons of information security and data protection:

* Websites that have a function for uploading information, unless this is necessary for valid business reasons;
* known or suspected malicious websites (e.g. those that spread malware or phishing content);
* Command and control server;
* malicious website obtained from threat data;
* Websites with illegal content.

Employees shall be trained in the safe and appropriate use of online resources, including access to the Internet. Training should include the organization's rules, the point of contact for reporting security concerns, and the exception process in the event that access to restricted web resources is required for legitimate business reasons. Furthermore, employees should also be trained not to disregard browser notices that report that a website is not secure but allow the user to continue.