

Security Policy   
Malware Protection

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Malware Protection | |  |
| 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 Content

[1 Principles 4](#_Toc187835205)

[2 Goals 4](#_Toc187835206)

[3 Controls 4](#_Toc187835207)

[3.1 Approved software installations 4](#_Toc187835208)

[3.2 Software to protect against malware 4](#_Toc187835209)

# Principles

SÜDVERS' IT systems must be protected against all forms of malware by using up-to-date malware protection software supported by effective procedures for dealing with malware-related security incidents.

# Goals

Protecting SÜDVERS from virus and malware attacks and ensuring that virus and malware infections can be dealt with within a defined time frame.

# Controls

Processes for approving the temporary or permanent disabling of some or all malware measures, including locations for approving exceptions, documented justification and review date must be defined and

## Approved software installations

Technical measures that prevent or detect the use of unauthorized software [e.g. application whitelisting] must be used for the respective IT systems used. e.g. application whitelisting) must be used

By means of regular automatic checks of the software and the data inventory of systems, in particular for systems that support important or critical business processes, the IT systems must be examined for unauthorized files (e.g. video files) or unauthorized changes (e.g. changes in the version status of the installed software) and any necessary corrective measures must be initiated

## Software to protect against malware

If technically possible and unless otherwise provided by the manufacturer, virus and malware protection software must be used on all IT systems that are exposed to malware, including

* Servers (e.g. servers that are at risk from viruses and malware, such as file and print servers, application servers, web servers and database servers)
* Gateway systems (e.g. e-mail gateway and web proxy servers that scan network traffic and electronic messages in real time) to minimize the penetration of viruses and malware into SÜDVERS' computer devices
* Computer devices (such as desktop computers, laptops and smartphones)
* Office equipment (such as network printers, photocopiers, fax machines, scanners and multifunctional devices (MFDs))

Where technically possible, IT systems must be hardened to minimize the impact of malware incidents. Further details can be found in the "Hardening" guideline.

Virus and malware protection software must protect against all forms of viruses and malware (such as computer viruses, worms, Trojans, spyware, rootkits, botnet software, keystroke loggers, adware and malicious mobile code)[[1]](#footnote-1) by providing at least the following functionalities

* signature-based malware protection
* heuristic malware protection

Anti-virus and anti-malware software must be updated automatically and within specified time periods (at least daily) to reduce the likelihood of IT systems being exposed to the latest viruses and malware (including those associated with "zero-day" attacks).

The virus and malware protection software must be configured to check at least the following:

* the computer memory
* the Master Boot Record (MBR) of hard disk drives
* targeted files (including executable files, image files such as JPEG, document formats such as Adobe PDF and macro files in desktop software)
* Protected files (e.g. compressed or password-protected files)
* Files that are read from or written to portable storage media (including drivers that must be installed when the corresponding storage media are mounted)

In addition to virus and malware protection on servers and end-user systems, an additional layer of protection based on an additional scanning engine, different from that of the endpoints and servers, must be configured at the Internet perimeter level to check for malware:

* Incoming network traffic (including emails and downloads from the Internet)
* Outgoing network traffic (including email attachments and shared documents).

Software for protection against viruses and malware must be configured in such a way that it:

* is active at all times
* Performs real-time scans of all read and write operations
* performs scheduled checks at predetermined times (complete check of local storage media at least once a month)
* Notification sent when suspicious malware is detected (e.g. by creating an event log entry and issuing a warning)
* Quarantines malware and all associated files immediately after detection
* ensures that important software settings for protection against viruses and malware cannot be deactivated or their functionality minimized by end users.

Regular checks of end-user devices must be carried out to ensure that:

* the malware protection software has not been deactivated
* the configuration of the malware protection software is correct
* updates are carried out correctly within the specified deadlines
* emergency procedures are in place in the event of a malware-related information security incident.

The risk of downloading malware must be reduced by:

* Restriction on downloading certain types of mobile code
* Configuration of web browsers so that users are asked whether they want to install mobile code
* Ensure that only trusted mobile code may be downloaded (e.g. signed with a trusted digital certificate)

For systems that are not technically or by design intended to run malware protection software, the following must be considered

* separation into secure network segments,
* Installation on special systems with low access rights,
* Software and service whitelisting and
* Further countermeasures

be taken into consideration.

Care must be taken to ensure that the maintenance and emergency procedures do not result in the introduction of malware that can circumvent the usual measures against malware;

1. It must be ensured that the configuration of the virus and malware protection software always follows the recommendations of the manufacturer of the application, database and operating system software running on the system. [↑](#footnote-ref-1)