

Security Policy   
Server systems

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Policy server systems | |  |
| 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 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](#_Toc107920650)

[2 Goals 4](#_Toc107920651)

[3 Controls 4](#_Toc107920652)

# Principles

Server installations (e.g. in data centers) must be designed to meet current and projected (foreseeable) business requirements for information processing and be protected by a range of built-in security controls.

The servers must be configured to function as required and prevent unauthorized or incorrect updates.

# Goals

Ensure that server installations can meet the security requirements of the applications they support (e.g. protection against compromising the confidentiality, integrity and availability of the information they process).

Ensure that the servers function as intended and do not jeopardize the security of computer installations or other environments.

# Controls

IT must have documented standards/procedures for the design of server installations that stipulate that:

* The safety requirements of SÜDVERS must be met
* The commissioning of the system must not lead to any negative effects on the operation of existing systems
* the protection of the intended systems and networks against unauthorized or malicious data traffic originating from other internal or external systems and networks is ensured
* information systems, networks and telecommunications facilities are designed in terms of their capacity and performance to meet current and planned developments in the use of IT by SÜDVERS.

The server installations must be designed in such a way that the following security architecture principles are taken into account:

* Inclusion of security in the project phases prior to the installation of new or fundamentally changed services
* Use of several layers of different types of protection (e.g. "defense in depth")
* Granting only the minimum access rights for users (e.g. "least privilege")
* Inclusion of a coherent, integrated set of technical standards
* Support for standardized naming conventions (e.g. computer/server addresses, network device names, device locations and user IDs)
* Minimization of individual sources of error (e.g. through load balancing, duplicate or alternative system components)

Server systems must have the following

* Sufficient capacity to cope with peak workloads
* Expansion/upgrade options to cope with anticipated demand
* a control and monitoring function.

Server installations must be designed in such a way that they:

* include the installation of software to protect against malware
* enable the creation of a predefined standard server configuration, the installation of which can be automated
* Enable authorized users to access multiple systems and resources via a single login (single-sign on)
* be managed from a central point
* Support the timely application of security updates (e.g. updates to access control lists (ACLs), signatures and firewall rules) to respond to changing threats, vulnerabilities and attacks as they occur.

Key components of server installations must be protected by separating critical business applications from all other business applications and information.

Live environments must be separated from the development and test environments by using different virtual servers and databases.

Servers must be configured in accordance with documented standards/procedures that include at least the following

* Provision of standard firmware configurations, if applicable
* Use of standardized, predefined server images to create/configure servers
* Changing the manufacturer's default settings and other security parameters
* Deactivation or restriction of unnecessary functions and services (see Hardening)
* Protection against unauthorized access
* Implementation of standard security management procedures.

Servers must be installed/configured using a standardized, predefined server image.

The server images must be regularly checked, tested and kept up to date (e.g. with the latest patches and changes to the build/configuration).

The servers may only be installed with the essential functions and configured in such a way that they are deactivated or restricted:

* non-essential or redundant services (such as Microsoft LAN Manager, X Windows, telnetd, fingerd, web browser and web server services)
* Communication services that are inherently susceptible to abuse (e.g. Server Message Block (SMB), SSH, tftp, RPC or rexec)
* Communication protocols that are susceptible to abuse (such as HTTPS, FTP, SMTP, Telnet and UUCP)
* Execution authorizations for sensitive commands or scripts (e.g. rlogin, rcp, rsh, remsh, tstp and trtp)
* Powerful system utilities (such as the Windows registry editor or sudo) or control panels
* Execution commands or command processors (e.g. Perl, Windows Powershell or Tcl)
* the function for automatic execution (e.g. from CDs, DVDs, portable storage devices and mounted/shared network folders).

Servers must be configured to protect the memory from misuse by malicious or compromised applications (e.g. by enabling Data Execution Prevention (DEP) and using Address Space Layout Randomization (ASLR) to prevent buffer overflow attacks).

Access to powerful system utilities and server parameter settings must be restricted to a limited number of authorized persons (e.g. system administrators)

The servers must be protected against unauthorized access by:

* Deactivation of unnecessary or insecure user accounts (e.g. the guest account (or an equivalent account) on Microsoft Windows and UNIX systems)
* Changing important security-relevant parameters (e.g. passwords) so that they differ from the default values specified by the manufacturers
* Calling timeout functions that automatically log off computer devices (that connect to the server) after a certain period of inactivity, clear screens and prompt users to log in again before the screens are displayed again.

Servers must be subject to standard security management practices that include the following:

* Restricting physical access to a limited number of authorized persons (e.g. by placing them in protected data centers or special, locked storage rooms)
* Maintain up-to-date malware protection software (including program code and signature files) to prevent infection by malicious software (such as computer viruses, worms, Trojans, ransomware, spyware, rootkits, botnet software and keystroke loggers)
* Use of a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools and backup software)
* Monitoring the systems (e.g. with the Simple Network Management Protocol (SNMP)) so that events such as hardware failures and attacks on the systems can be detected and responded to quickly and effectively
* Use of secure technologies such as SSH, S-FTP, TLS or IPsec VPN to protect insecure services such as NetBIOS, file sharing, Telnet and FTP
* updates to keep them up to date (e.g. by applying approved procedures for change management, vulnerability management and patch management)
* Regular checks to verify configuration settings, assess password strength and evaluate the activities performed on the server (e.g. through automated evaluation of application logs and event logs as part of a SIEM solution).