

Security Policy   
Remote Access Infrastructure

Information security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Remote Access Infrastructure | |  |
| 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 | |
| Scope of application | SÜDVERS Group | |
| 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 Principle 4](#_Toc137726121)

[2 Objective 4](#_Toc137726122)

[3 Controls 4](#_Toc137726123)

# Principle

The ability to work from remote locations is essential for SÜDVERS employees. Connection options must therefore be provided to enable connections from outside SÜDVERS to SÜDVERS systems (e.g. via VPN connections).

# Objective

It must be ensured that all SÜDVERS employees are able to access defined company resources from outside the company network in a secure manner using IT systems that are approved or fully controlled and managed by SÜDVERS.

# Controls

Remote access to SÜDVERS systems that are not located in the designated network zone (external DMZ) is only permitted for secure systems via predefined and agreed connection methods. These methods include (but are not limited to):

* Site-to-site VPNs
* used for connections from/to third-party providers or business partners
* Dial-up VPNs
* Are used for secure endpoints by SÜDVERS employees or third-party providers
* Terminal servers, Citrix, CyberArk and VDIs
* Are used to enable SÜDVERS employees or third-party providers to connect to SÜDVERS systems, regardless of the end-user system used
* Cloud-based authentication systems (such as SÜDVERS MS Azure AD)
* Are used to support SSO authentication

IT systems and networks that are accessible via external connections over insecure networks must (not limited to)

* are located in secure network segments that are protected by stateful inspection firewalls
* be protected by network-based intrusion prevention systems
* installed on dedicated systems that are not running on the same hosts used to provide services used for other purposes
* Restrict external network traffic to certain parts of IT systems and networks
* Restrict connections to certain access points (e.g. certain network gateways)
* for non-VPN connections, check the source of the external connections (e.g. by checking the source IP address or the system certificate)
* Log security-relevant activities
* Log details of established external connections (e.g. Internet or VPN)

IT systems that are accessible via insecure external connections must also be subject to strong authentication, whereby the first authentication stage must be carried out by a system before the actual target system is reached.

Remote access by employees to SÜDVERS systems via (dial-in) VPN connections must be restricted to devices that meet the minimum security configuration requirements, including checking that the devices are

* being authorized
* up-to-date malware protection is installed
* the latest approved systems and software patches are installed
* an up-to-date personal firewall and a host-based intrusion prevention system with a predefined standard configuration is used
* They are configured so that they do not allow routing between the network segments to which they are connected (and do not allow split-tunnelling).

For remote access to critical environments, active individual authorization (e.g. via a PAM system) and time-based access should be considered.

All network connections used for remote access must ensure compliance with the network connection policy. It should be borne in mind that a connection from a third-party IT system can have a maximum trust level that allows it to end in an internal DMZ.