

Security Policy   
Customer connections

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Customer Connections | |  |
| 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 contents

[1 Principle 4](#_Toc138053219)

[2 Objective 4](#_Toc138053220)

[3 Controls 4](#_Toc138053221)

# Principle

Customer access to business applications must be clearly identified, recorded in an inventory of connections, protected by access control mechanisms and monitored.

# Objective

Protection of the confidentiality, integrity and availability of critical or sensitive information concerning either SÜDVERS or the customer.

# Controls

IT must have documented standards/procedures in place to define the technical security measures for customer connections, which include the following

* the provision of access control mechanisms for customer access
* Protecting the integrity of critical information and the confidentiality of sensitive information
* Management of customer connections

Customer access control requirements must be defined to protect critical and sensitive information and include

* Authorization of persons before they are granted access to business applications
* Access authorizations required for access to business applications or certain functions in a business application
* Access control mechanisms (such as passwords, tokens or biometric data)

Access controls for business applications must be strengthened by using the following

* Multi-factor authentication (e.g. a combination of password, token and/or biometric method)
* the use of authentication hardware, such as physical smartcard readers, physical tokens or smartphones
* additional information to verify the origin of access (e.g. through location-based authentication that uses the IP address as geolocation, GPS or positioning in the mobile network)
* Systems to ensure that the connecting computer device is trustworthy/known.

The integrity of critical information and the confidentiality of sensitive information must be protected by:

* Encryption of information during transmission
* the use of digital signatures so that transactions and messages cannot be refuted (e.g. non-repudiation)
* additional authentication for sensitive transactions or procedures (e.g. payments or transfers of large amounts) to prevent attacks such as man-in-the-middle attacks.

Customer access must go through a sign-up process before access to business applications is granted, which includes the following

* Perform integrity checks to ensure that connected devices have not been compromised by malware (including computer viruses, worms, Trojans, spyware, rootkits, botnet software, keystroke loggers, ransomware and malicious mobile code)
* Display of contractual conditions that limit the liability of SÜDVERS towards customers (e.g. through the use of warning notices on the screen).

Customer access to business applications must be protected (according to the principle of least access) by:

* Restriction of connection methods (e.g. to certain remote access devices or access points and only via firewalls)
* Configuration of information systems and networks to restrict access (e.g. to specific IP addresses or an IP range)
* Restriction of the type of access granted (e.g. in relation to permitted information, application functions and access rights)
* Timely termination of customer connections (e.g. after a certain period of inactivity, in the event of a security breach or when they are no longer needed)