

Security Policy   
Access control

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Access control | |  |
| 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](#_Toc141096879)

[2 Objectives 4](#_Toc141096880)

[3 Controls 4](#_Toc141096881)

[3.1 Access control 4](#_Toc141096882)

[3.2 Authorization of users 7](#_Toc141096883)

[3.3 Access control mechanism 7](#_Toc141096884)

[3.4 Registration process 8](#_Toc141096885)

[3.5 Regulations for emergency situations 8](#_Toc141096886)

[3.6 Exceptions 9](#_Toc141096887)

# Principles

Access control measures must be put in place to restrict access to business applications, IT systems, networks and computing devices for all types of users, who must be given specific privileges to restrict them to certain information or systems.

# Objectives

Ensure that only authorized individuals have access to business applications, IT systems, networks and computing devices, that individual accountability is ensured and that authorized users are provided with access rights that are sufficient to perform their duties but do not allow them to exceed their authority.

# Control en

## Access control

Access to business applications, IT systems, networks and computer devices as well as the information stored and processed on them must be restricted to authorized persons and IT systems.

Access control must be managed according to a multi-layered concept, distinguishing between access to system resources (e.g. access at operating system level, which must be granted by the system owner) and access to data (e.g. access rights within business applications, which must be granted by the information owner).

Strong authentication mechanisms based on relevant standards and special control systems must be used for access control.

Access control must:

* access
  + For all types of persons (e.g. business users, system operators, IT specialists, e.g. technical support staff, and persons from external parties)
  + For all types of automated IT systems that require access to systems or information (e.g. service or system accounts)
* can be applied to all types of information, systems and software (e.g. current business information, application and system software, access control data, backup files and system documentation).

The access control measures must:

* map the access restrictions in accordance with the access rights granted by the owners of the business applications and IT systems
* restrict the system functions that can be accessed (e.g. by providing menus that only allow access to the specific functions required to fulfill a particular role)
* minimize the need for special access rights (e.g. UserIDs that have additional capabilities, such as "Administrator" in Windows systems, or special capabilities, such as UserIDs that can be used to authorize payments)
* minimize the need to share accounts. If technically possible, no group accounts or shared accounts may be used
* Ensure that access rights are granted in such a way that users can perform the required maintenance tasks (e.g. adding/changing printers, connecting to the wireless network and changing the relevant configuration settings, etc.)

The access control regulations must be regularly

* at least every twelve months for SÜDVERS employees without special access authorization
* at least every six months for users with special access rights (such as system administrators, super users, ...) or for users with access to data protection-relevant information (HR department, ...)
* at least every three months for users of third parties or temporary staff (e.g. contractors, 3rd party providers...)

be checked:

* to ensure that access authorizations remain appropriate
* to check whether superfluous authorizations have been deleted (e.g. for people who have changed their role or left the company)
* in response to new and evolving threats, capabilities, vulnerabilities, business requirements or information security incident experience

Access rights must be approved by a sufficiently senior company representative.

Before the access authorization comes into effect:

* The authorizations must be checked by the respective line organization to ensure that the access rights are appropriate.
* Details of the users must be recorded, including their true identity, the associated identifier (e.g. UserID) and the access authorizations to be granted
* Users must be informed about their access rights and the associated terms of use and must confirm that they have read them.

Access rights must not be assigned collectively (e.g. using identifiers such as UserIDs or authenticators such as passwords that are shared in a group) unless there are special circumstances. If collective assignment of access rights is required, this must be documented, approved by a responsible company representative and subject to additional controls (e.g. use of PAM solutions).

For special access rights (such as "root" in UNIX or "administrator" in Windows systems, i.e. rights that can be used to authorize payments or perform financial transactions or that include access to privacy-sensitive information), additional controls must be implemented that include the following

* Specification of the purpose of the special access rights
* Ensure that end users are not given access levels that can be used to change the security configuration
* Users with special access rights must log in with a different user account than under normal circumstances
* Regular (e.g. quarterly) logging and review of the use of special access rights
* Keeping a register of accounts with special access rights.

A procedure for changing the access rights of users must be set up to ensure that, if necessary:

* the authentication data and access rights be changed immediately on all systems to which the user had access
* Access profiles/accounts can be changed
* components that enable access, such as tokens, modems or virtual private networks (VPNs), can be replaced if necessary.

A procedure for terminating users' access rights must be established to ensure that, where necessary:

* the authentication data and access rights on all systems to which the user had access are withdrawn immediately if they are no longer required (e.g. when changing roles or moving to another area of SÜDVERS or when leaving SÜDVERS)
* the login data is deactivated
* Access profiles/accounts are deleted
* Components that allow the user access (such as tokens, modems or VPN access) can be deactivated or removed.

## Authorization of users

The processes for authorizing users must:

* be documented in writing and apply to all users
* link access rights to defined users (e.g. by using unique identifiers such as UserIDs)
* Assign standard access to users according to the principle of least privilege (e.g. "none" instead of "read")
* ensure that redundant identifiers (such as UserIDs) are not released for use again
* Assign 3rd party users with access rights
  + which have a maximum validity of 1 year[[1]](#footnote-1)
  + that, if the duration of the required access is not known, there is a maximum validity of 30 days
* ensure that emergency situations arising from security incidents can be managed.

A database must be set up with details of all authorized users for each system (e.g. Microsoft AD), which is maintained by designated persons, e.g. certain system administrators, and protected against unauthorized changes and unauthorized disclosure.

## Access control mechanism

All users must be authenticated by a unique identifier (such as a user ID) and an authenticator (such as a password (sometimes referred to as a passphrase, passcode or PIN code)) before they are granted access to critical or sensitive business information, business applications, operating systems and computing devices.

Details on the use of passwords and password requirements can be found in the corresponding SÜDVERS password policy.

There must be a procedure for assigning new or changed passwords that:

* verifies the identity of the user who is to receive the information
* directly involves the person to whom the password clearly applies (e.g. personal registration at a secure location or by registered mail requiring proof of identity and the person's signature)
* ensures that the user is notified when passwords are about to expire

## Registration process

The login mechanisms must be configured in such a way that they:

* only validate the login data if it has been entered completely
* limit the number of permitted unsuccessful login attempts (e.g. to eight attempts within 4 hours before the user account is deactivated for a predefined period or until the IT helpdesk is authorized to activate the account)
* Limit the number of simultaneous sessions of a user (by default, a maximum of 2 per end user is allowed
* Limit the duration of a user's login session
* be reactivated automatically after an interruption (e.g. if the logon process is required again after disconnecting from the application).

The login mechanisms must be configured to provide information so that they:

* warn that only authorized users have access
* Record all successful and unsuccessful login attempts
* inform highly privileged IT users about the date/time of their last successful login and all unsuccessful login attempts since their last successful login.

The login mechanisms must be configured in such a way that the authentication data is protected against unauthorized disclosure by:

* use cryptographic hashing algorithms to obfuscate plaintext passwords and protect against brute force attacks
* Use salting methods to ensure that each password hash is unique to resist attacks with rainbow tables.

The approval of both the line organization of the information owner, the IT manager and the information security organization must be obtained before important functions of the logon process are bypassed, deactivated or changed.

## Regulations for emergency situations

In declared emergency situations, authorized employees and external emergency services must be able to override security controls. The corresponding processes must be documented and approved on a case-by-case basis by the IT management and information security organization.

Once the emergency has ended, normal operation and the corresponding safety controls must be restored.

## Exceptions

General exceptions to this guideline can be applied for (after consultation with the respective superiors) by the system managers and the heads of the specialist departments.

Exemption requests for certain individual systems must include documentation of a risk assessment performed, documented mitigation measures and proposals for alternative controls.

All exceptions must be approved by the SÜDVERS Information Security Officer.

General exceptions are recorded in this section of the document. Specific individual exceptions are documented as part of the system documentation.

The following exceptions to the directive apply:

* Requirements regarding regulations for emergencies (existence of local accounts, ...) apply from 1.7.2023
* Requirements regarding non-repudiation with regard to the use of system and service accounts will be implemented as part of the introduction of a PAM solution and will therefore only apply from 1.1.2024

1. Can be extended as part of the access verification process [↑](#footnote-ref-1)