

Security Policy   
Passwords

Information Security

|  |  |  |
| --- | --- | --- |
|  |  | |
| Passwords | |  |
| 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 contents

[1 Principle 4](#_Toc167360298)

[2 Objective 4](#_Toc167360299)

[3 Controls 4](#_Toc167360300)

[3.1 Password rules 4](#_Toc167360301)

[3.2 Guidelines for password protection 6](#_Toc167360302)

[3.3 Specifications for application development 7](#_Toc167360303)

# Principle

For business applications, IT systems or networks that are configured with a password-based access control mechanism, users must provide a valid user ID and password before they can gain access to these systems.

# Objective

To prevent unauthorized users from gaining access to password-protected business information, business applications, IT systems, networks, target environments must be configured with password-based access control mechanisms to ensure that users can only gain access to them by providing a valid UserID and password.

Since not all systems support certificates or one-time tokens, every user needs to know

* How to choose secure passwords
* what the requirements for secure passwords are

# Controls

Users of access control systems that are based on passwords must

* use strong authentication mechanisms[[1]](#footnote-1) , which are based on relevant standards and special control systems
* treat their passwords confidentially. If it is technically necessary for users to save their passwords, the use of encryption is mandatory.
* change their passwords immediately as soon as they discover that they have been compromised
* notify the IT helpdesk if passwords have been compromised or are suspected of having been compromised.

## Password rules

As far as technically possible, the following rules apply:

* The use of shared accounts (unless technically necessary) or the sharing of passwords with others is prohibited.
* A secure password is mandatory, which means that passwords
  + must be unambiguous
  + differ from the user ID
  + if strong authentication is used for the account, at least eight (8) characters, for the accounts for which strong authentication is not available or is not used for legitimate reasons, at least thirteen (13) characters long
  + contain at least one character from each of the following categories:
    - Lower case letters (a-z)
    - Capital letters (A-Z)
    - Numbers (0-9) or special characters (!@#$%^&\*()\_+|~-=\`{}[]:";'<>?,./)
* The minimum age of passwords is set to at least 1 day.
* Saving passwords with "Reversible Encryption" must be deactivated.
* After 8 unsuccessful attempts, the account must be blocked to prevent misuse
* The option "Duration of account blocking" must be set to 0 minutes.
* The "Reset account lockout counter after" option must be set to at least 240 minutes

Additional requirements for passwords used by people with full access to the operating system level of multi-user or server systems, for local system accounts known to multiple people, for general system-level passwords, or for service accounts that can be used for interactive login:

* The minimum password length is set as follows:
  + if strong authentication is used for the account, at least eight (8) characters,
  + for the accounts for which strong authentication is not available or is not used for legitimate reasons, at least twenty (20) characters
* The maximum validity period of a password is set as follows:
  + if strong authentication is used for the account, no need for a change
  + for the accounts for which strong authentication is not available or is not used for legitimate reasons, at least every 90 days.
* After 3 unsuccessful attempts, the account must be blocked to prevent misuse.
* Passwords for service accounts must be stored in a secure location and may only be made available to those who need access to these accounts in order to ensure system operation.
* Passwords for general system or service accounts that can be used for interactive login must be changed immediately if a person who knows this authentication data leaves the company or takes on a new task for which this knowledge of the authentication data is no longer required.

Administrators of IT systems and applications as well as members of system or user support are responsible for ensuring the following within their area of responsibility:

* As far as technically possible, the password is not displayed in plain text when logging in.
* Passwords are masked
* passwords and associated PIN numbers (if available) are protected during storage and transmission
* passwords are changed immediately if there is a suspicion that they have been compromised or illegally disclosed
* Initial passwords are unique for users and cannot be guessed
* The password is communicated to the user in a secure manner.
* After the first login or password reset, users are prompted to change their password.
* The identity of the user/caller is verified by the IT helpdesk before resetting passwords or processing requests in connection with the activation or unblocking of accounts.
* The initial temporary user password is linked to a user's unique identifiers and cannot be guessed.
* Critical IT infrastructure and application passwords must be changed immediately after security incidents that have led to the compromise of authentication information, or the associated user accounts must be deactivated.
* The default passwords of systems or providers are changed immediately after configuration or commissioning of the system.
* During the login process, the authentication information is transmitted over the network in encrypted form.

## Guidelines for password protection

Users may not use the same password for SÜDVERS accounts and private access (such as personal accounts, options trading, internet forums, etc.).

If it is suspected that an account has been compromised, users must report the incident to the IT helpdesk and change all relevant passwords.

An attempt to crack or guess passwords can be carried out by the information security officer on a random basis. If a password is guessed or cracked during one of these checks, the user must change it.

Requirements for changing passwords: (with the exception of passwords at operational and system level, which must be changed in accordance with the specifications)

* Passwords must not be reused under any circumstances.
* Users must change their passwords immediately after logging in to the applications/IT systems for the first time.
* Users may not pass on their passwords.
* Passwords must not be encoded/stored in programs or IT systems (including mobile and wireless devices) in plain text.

## Specifications for application development

Application developers must ensure that their programs contain the following security precautions:

* You must support Single Sign On.
* You must support the authentication of individual users.
* Passwords must not be stored in plain text or in an easily reversible form.
* They should support role-based access controls so that one user can take over the functions of another without knowing their password.
* In the case of expiring passwords, a message should be sent to the user in good time before the expiry takes effect.

1. Strong authentication" is a standing technical term in information security and the technical form based on the respective state of the art (the requirements for this are therefore constantly increasing). In general, it can be said that, as things stand today, the following counts as strong authentication (in addition to username and password): Use of biometric authentication, use of certificates for authentication, use of MFA (e.g. with the help of Microsoft Authenticator). [↑](#footnote-ref-1)