Titel:	**Password Policy**

1. Objective and purpose

The guideline regulates the allocation, design and handling of passwords used for the authentication of authorized users. The guideline is based on the NIST standard (800-63B).

2. Terms

Terms (in alphabetical order)**:**	**Explanation:**

3. Responsibilities

The IT department is responsible for implementing the policy and monitoring compliance.

4. Scope of application

These guidelines apply to all companies belonging to Bauerfeind AG as well as to all users of IT systems that are supported or provided by Bauerfeind AG. It obliges all users of IT systems to comply with the specifications set forth here.

5. Obligations of the users

- Passwords may only be known to the user personally and may not be disclosed to third parties.
- A separate password must be used for each IT system or application.
- Passwords that are easy to guess or are listed in common password[1] lists must not be used. In particular, the following are to be avoided:
  - Information from the personal or professional environment of the user such as names, names of relatives, vehicle registration numbers or dates of birth
  - Character repetitions
  - Character(s) that are entered by adjacent keys like 123456... or qwertz/qwerty...
  - simple number and letter combinations
  - character combinations that differ only slightly from the previous passwords
  - Character combinations that correspond to search terms in dictionaries and encyclopedias (trivial passwords)
- Passwords may only be entered unobserved.
- Passwords must not be stored on programmable function keys of keyboards or mouse.
- A password may only be set in writing for an emergency deposit. In this case, it must be stored securely, e.g. in a safe or a password manager with secure encryption.
- A password must be changed if it has become known or is suspected to be known by unauthorized persons.
- Normal office activities must be performed with non-privileged accounts. For privileged activities a separate personal account is to be used. The allocation of privileged accounts requires an inquiry and is done by the IT department.

6. Control of password quality

- The minimum length for passwords is 8 characters

  The length of a password is significant responsible for the security. For this reason, it is recommended to use **more characters** for a secure password.
- The maximum length for passwords is 64 characters.
- Passwords must consist of a combination of uppercase letters, lowercase letters, numbers and special characters.
- Passwords must be changed every 180 days.
- For publicly accessible systems or when authentication is performed over a public or insecure network, **Multi-Factor Authentication** must be used.[2]
- The PIN of a smart phone/tablet has the same length requirements as a password.[3]

  The use of biometrics (e.g. fingerprint, face recognition, etc.) is recommended to increase ease of use and reduce the frequency of entering PINs on the smartphone/tablet.

[1] https://en.wikipedia.org/wiki/List_of_the_most_common_passwords
[2] The implementation is done by the IT department, users are instructed in advance.
[3] The required length is specified by the IT department.