Password Policy

Christian-Albrechts-Universität zu Kiel
Rechenzentrum

July 2017

Preamble

Many systems and data files at Christian-Albrechts-Universität Kiel (CAU) are protected with user/password combinations. These passwords are for protecting business data and for protecting your personal data from insight or modification by unauthorized persons. For providing this confidentiality the Computing Centre determines minimum requirements for passwords. This guideline applies to all CAU members, who use IT services and supplements the binding "User Framework Regulation" for communication and data processing structure at Kiel University.

Goals

The goal of these rules is to increase the security level and prevent from brute force attacks. For achieving an appropriate protection level, passwords need to be in accordance with the relevant minimum requirements regarding lack of structure / randomness / complexity. Please note that technical guidelines do not prevent from revealing passwords to unauthorized persons (e.g. phishing attacks). Thus, please handle your passwords with care.

The following rules are minimum requirements for regular activities. In case you work with confidential or personal data or your data has a special need for protection, please choose a longer password when in doubt.

Password structure

The password may contain characters of the following four groups:

- Lowercase letters: `abcdefghijklmnopqrstuvwxyz`
- Uppercase letters: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`
- Digits: `1234567890`
- Special characters: `!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~`

Please note, that for technical reasons the list does not contain any umlauts, ß, spaces and no further special characters such as § or °.

The minimum length of the password depends on how many of the above mentioned character groups are used and has to be

- **14 characters**, in case only uppercase or lowercase letters are used. Passwords containing only digits or only special characters are not allowed.
- **12 characters**, in case characters from an additional group are also used, e.g. lowercase letters and digits or uppercase letters and lowercase letters.
- **10 characters**, in case characters from three of the above mentioned groups are used, e.g. uppercase letters, digits and special characters.
- **9 characters**, in case characters from all of the above mentioned groups are used.

The above mentioned lengths are minimum requirements, for establishing the security level of a randomly generated password (e.g. „NR27ſHUpſG“). A password that consists of „sensible“ words should be at least 50% longer than recommended above. In addition to this, the Computer Centre reserves the right to keep a blacklist with easy-to-guess password components (e.g. „password“ or „1234“), which are not allowed to be part of the password.

Unfortunately, these guidelines cannot be applied to all available systems (e.g. because of a length restriction to 6 characters for passwords). In this case, please try to follow the guidelines as good as possible, for example by choosing the maximum password length and a random choice of all allowed character groups.

Changing passwords

Due to the sufficient amount of randomness we do not consider it necessary to change your password on a regular basis. Nevertheless, please change your password immediately if one of the following cases applies:

- You are afraid that your password is no longer secret because,
  - You already entered it on a device which might be not trustworthy (e.g. computer virus or malware infection),
  - You accidentally clicked on a link in an email which then directed you to a password change,
  - You have lost an old hard drive or a mobile device on which login data were still saved, or the device has not been disposed in a proper way. Please note that it is generally possible to retrieve data from broken devices!
- Your password has been reset for you.

Safe handling of passwords

The fact that your password is protected against brute force attacks does not mean that there is no danger of physical or digital password theft.

- Please do not enter your password on a device you don’t trust!
- Please do not save your password unencrypted on your pc or mobile device!
- If possible, please use a master password in your application system.
- Do not reveal your password to others! Computing Centre employees will never ask you for your password! Never click on email links, in which an unexpected password change or confirming your account is requested!
- In case you store your password in written form, please do this in a safe place, e.g. in a closed envelope which is in a locked file cabinet or in a safe!
- When you receive a new password, please change it immediately for ensuring that only you know the valid password.

- Please do not use the same password for several accounts or service providers! There are numerous (also free-of-charge) password management systems, which assist you managing your passwords. Further information can be obtained at the Computing Centre website.

Computing Centre CAU, 06.07.2017