Goethe University recommendations and best practices for handling passwords

The following recommendations apply to all members of Goethe University Frankfurt. They regulate the secure use of passwords. Goethe University regulations and statutes, in particular IT security regulations, IT security guidelines and the IuK use regulation[1], are not affected by these recommendations.

Data in a system must be protected, and be accessible to authorised persons only. This can be accomplished through personal chip cards, by monitoring biometrical characteristics (e.g., finger prints) or by entering a use name and a password. Card-supported and biometrical login processes are growing in significance, but logging in with a username and password remains the predominant method. This guideline outlines how to achieve the most secure password protection possible.

If someone else learns your username and password, they can log in with your name and access data and programmes not intended for them. Since usernames are seldom concealed, it is essential that personal passwords are kept secret.

Goethe University's Security Management Team (SMT) recommends the following rules for choosing passwords:

1) A password length of **16 characters** is advisable; but it should at least have a minimum of 10 characters.

2) A password should include a mix of capital and lower case letters, numbers, and preferably **symbols** as well.

3) One way to create a password of the required length that is also easy to remember is to link two or more ***unconnected (!)*** words with random symbols strewn in between.

4) If for technical reasons only shorter passwords are possible, priority should be placed on a high degree of **randomness** of characters. This can be achieved by memorising a sentence, taking the first letters of those words and then inserting symbols in suitable places.

5) A password should not be easy to guess, for example username, first or last name, license plate number, or birth date.

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt – General use regulations for information processing and communication infrastructure at Goethe University Frankfurt

6) Passwords must be kept **secret** and changed regularly. **Passwords used officially** may **not** be used for external services.

7) One password should be used for one place only. Such passwords can be easily remembered by placing different characters in front of a frequently used chain of characters, for example: "`GUHier2Mond%Kachel`", "`1aHier2Mond%Kachel`",...

8) **Email logins** should be particularly well-protected, as they can be used to change to all other passwords. In no case should passwords be used that are also used in other places.

9) The following are **examples** of secure passwords (do not use these examples as your password under any circumstances as they can now easily be tested…):

```
Hier2Mond%Kachel
6uybi+sY
msJ$DR8Ttx
…
```

10) **Password managers,** i.e., programmes that store passwords help with managing the use of many different passwords. The password managers provided by web browsers should only be used if they have separate password protection given by the user. External programmes are preferable.

11) If you suspect that unauthorised persons have learned your password, or if a **system compromise** is suspected, **change your password** immediately. In this case, please contact the administrative or IT security officer in charge immediately. You can change **your HRZ password** at this link: https://kartenservice.uni-frankfurt.de/mitarbeitercard/password

12) Please contact your IT support or your IT security officer if you have any questions.

Further information:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) - (Federal Office for Information Security)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) - Goethe-University IT Security Management Team
  https://www.uni-frankfurt.de/smt

- Goethe University Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) – Goethe University Computing Centre
  https://www.uni-frankfurt.de/hrz/it-sicherheit