INFORMATION SECURITY

20 June 2016

Information sheet: Good passwords

A good password ...

- comprises at least 8 (and ideally 10 or significantly more) characters
- contains at least two letters, using both uppercase and lowercase
- contains at least two numbers or special characters, where possible not just at the beginning/end
- is easy to memorize
- can be typed quickly (without being seen by someone looking over your shoulder)
- does not follow a (discernible) system, i.e. appears to be random
- is not a word in a known language
- is only known to the password owner

Multiple usernames

As a general rule, you should choose different passwords for different usernames. If you have several usernames and must therefore memorize multiple passwords, we advise creating systematic password families. This means a passwords comprising 6–7 characters, which can then be supplemented with 1–2 characters that allow you to differentiate between the different usernames (computer name or purpose of the protected application). Another option for managing multiple passwords is a password safe, that is, a program that stores passwords in a highly encrypted database. This must then be protected with a particularly strong password.

Rules for creating a password

There are several ways to create a password. The following always applies: Don't memorize the password, but rather the method used to create it!

For an overview of common password formation rules, see the RRZ website:
https://uhh.de/rrz-passwortregeln

In case of questions or suggestions on this topic, contact the RRZ ServiceLine by telephone (+49 40 42838-7790) or via email (rrz.serviceline@uni-hamburg.de).