Password Policy

The institute uses a central account checking service for all computer related tasks (Kerberos). You can access the AFS directory, the wiki, version management, and various other services all with the same login. Some of these services are usable from the general internet. Please treat your personal login as diligent as you do with your transponder.

How to change passwords

There is a dedicated URL that can be reached from within the institute:

https://password.iqo.uni-hannover.de/

This interactive form requires you to give your current password for authentication. If you can't remember your current password, please contact one of the computer admins of the institute. They technically cannot tell you your password, either. But they will gladly provide you with a new one. Remember, in terms of computer security, a forgotten password is better than a password scribbled on a piece of paper.

General Password Rules

We trust you to follow these general rules:

- Passwords shall not be disclosed to anyone
- Passwords shall not be used for non-IQO services. No password recycling, please.
- Do not keep the password written on a note in an obvious place (in your purse, in a drawer of your work place, a file, ...)
- Never communicate a password by telephone, e-mail or instant messaging
- Make sure, you log off or lock screen before leaving a computer unattended

Requirements for a password

There are some requirements that are automatically enforced when setting the password:

- The password must be at least eight characters in length.
- The password must contain characters from at least three of the following four categories:
  - Upper case letters
  - Lower case letters
  - Numbers
  - Special characters
- The password must not contain three or more consecutive characters from the name of the user.

Recommendations for the choice of a password

- Do not include your own userid – this is very weak and can easily be guessed.
- Do not include your own first name
- Do not include your last name
- Do not include names of persons associated with you – no spouses, friends, etc…
- Do not include the name of your project, or well known abbreviations of your work (iqo, bec etc.)
- Do not use real words. There is malware that systematically tries each and every word in common dictionaries, and/or slight variations.
- Do not use Umlaut characters. You'd be in trouble if you want to login from computers with non-german keybord layout
- Do not use space as the last character in a password. This is not supported by the Network Identity Manager. But still works with command line log in.

Password generator pwgen

Password generators save you the trouble to invent password that fulfills the above constrictions. Some even manage to come up with passwords that are easier to remember than purely randomly diced characters. One well known password generation tool is pwgen.

- pwgen is packaged in every major linux distribution
- a binary for Windows can be downloaded from http://pwgen-win.sourceforge.net/
- a binary for MAC OS that includes a nice GUI is available from http://www.macupdate.com/app/mac/33085/pwgen
- there even is a plug-in for firefox: https://addons.mozilla.org/en-US/firefox/addon/pwgen-password-generator/