Regulations for the use of computer systems, effective 27 January 2009

The undersigned hereby confirms that he/she accepts the following obligations relating to the use of the computer infrastructure provided to students at Neu-Ulm University of Applied Sciences, in particular the computer rooms, lecture halls and facilities of IT Services.

1. Network, hardware and software

- Users must conduct themselves in such a way that the IT systems can be operated and used without disruptions. Technical equipment and resources (disk space, peripherals, consumables) must be treated with care and used in an economical and responsible manner.
- Computers and peripherals may not be opened up without authorisation, and no actions are permitted that interfere with normal operations.
- Users must immediately report any deficiencies, such as technical faults, information received by mistake or security holes. They must also report any programs that show signs of malfunction (virus, root kit, etc.).
- Privately owned laptops that are connected to the university network via LAN or WLAN must have an up-to-date virus scanner and operating system. Additional information on virus protection can be found in the instructions for computer services. The firewall must not be shut off, and sharing of directories or services must be deactivated or at least protected by strong passwords.
- Installation of software and changing of system settings are not permitted at PC workstations. If you need additional software or hardware, please contact the IT Services staff.
- Copies may not be made of software provided by the HNU. Modification of programs, decompilation and other attempts to discover the source code are prohibited.

You must familiarise yourself with the software licence agreements, adhere to them and comply with all provisions contained in the law (copyright).
- You are not allowed to eavesdrop on network traffic or record it.
• You are not allowed to connect to the network or Internet using any means other than those provided by the HNU (modem, Wi-Fi hotspot, etc.).
• Instructions issued by HNU staff must be obeyed.

2. Data

• Users are responsible for the content of their e-mail messages and websites. Documents and files with objectionable content must not be made available on or requested from computers and networks of the HNU.
• Users are responsible for backing up their own data on the H drive and on their local PCs.
• The Internet and its services must be used only for study purposes.
• I consent to inclusion of my email address in the HNU’s main address book and distribution lists.
• I consent to software checks for spam and viruses on all e-mail messages sent to my HNU email address. This has the following consequences:
  1.) Emails with viruses or critical attachments will automatically be placed in quarantine and can be delivered only by IT Services. You will be notified by email if you have any messages in quarantine.
  2.) Emails with a very high spam probability will be deleted immediately. Emails with a high spam probability will no longer be delivered to your inbox. Instead they will be placed in quarantine. You will receive an email each week informing you of messages in quarantine (if there are any). This email will contain a link to the quarantined spam messages. You can select the messages that you want to have sent to your inbox (this does not apply to messages with viruses or illicit attachments).

Any messages in quarantine which you do not delete yourself will be automatically deleted from the quarantine folder after 21 days
• If you notice any irregularities in workstations, programs or data, report them immediately to IT Services.
• If you want to process personal data, discuss this with the Data Protection Officer in advance. You must comply with all the provisions of the German Federal Data Protection Act.

3. Computer access

• Choose secure passwords and keep them to yourself.
• Do not disclose your passwords to others. If someone asks you for a password, refer him or her to the responsible administrators. There are very few cases in which your password is needed for IT support. However, if a password is actually needed for this purpose, enter it yourself and watch while the work is being carried out.
• Do not use other people’s passwords.
• Do not leave insecure IT systems unattended.
• Remember that you are responsible for whatever is done using your user name and password.
• It is prohibited to spy on passwords or use other people’s access authorisations. If you find out someone else’s password, report this to the IT Services staff.
• It is forbidden to copy or modify data from third parties without their permission.

If you abuse your access rights or violate these regulations, your right to use the computers can be suspended or restricted.

Email is one means by which the HNU sends out important messages and announcements. These messages are sent to the mailbox corresponding to your user account. We advise you to manage your mailbox and check it regularly so that you can be quickly reached at any time.

When a user account is closed (deregistration), the user’s account, mailbox and data are deleted from the central servers. The printing account is also closed. Amounts remaining on the printing account will not be refunded.

A person who fails to comply with these regulations is subject to official measures pursuant to Art. 18 (1) of the Bavarian Higher Education Act (BayHSchG) and Section 14 of the Enrolment Statutes. Serious infringements may result in damage claims under civil law and/or criminal prosecution. It is expressly pointed out that the following acts are punishable under German law:

• Data espionage (Section 202a StGB [German Penal Code])
• Unlawful alteration, deletion, suppression or rendering unusable of data (Section 303a StGB)
• Computer sabotage (Section 303b StGB) and computer fraud (Section 263a StGB)
• Dissemination of propaganda from unconstitutional organisations (Section 86 StGB) or of writings which incite hatred against a racial group (Section 130 StGB)
• Making accessible and disseminating certain kinds of pornography in the network/internet (Section 184 StGB)
• Offences involving insult such as verbal abuse or defamation (Sections 185 ff. StGB)