

Hochschule für Technik Stuttgart

User Regulations for Network Operations

1. The user receives his/her own disc storage area named hereafter "account", which is to be protected by a password.
2. The user should regularly alter his/her password. The password should contain letters and numbers, as in the example „jack89rabbit". No dictionary terms should be employed without numbers.
3. Only the user who has signed for the account is allowed to gain access to the account. No one else is allowed to use the account or to know the access-account password.
4. Upon completion of one's tasks with the computer network, the user has to log out.
5. It is forbidden to use the computer network or data received through the network for commercial purposes.
6. Technical defects, unintentionally received messages or recognised security gaps must be reported to the Rechenzentrum (EDPC = Computer Center) immediately.
7. Any abuse of the computer network is strictly forbidden. In particular the following practices are not allowed:
 - a. Use of the network services, whenever the behaviour of the user violates protective legislation (e. g. criminal laws, youth-protection laws, data-protection laws).
 - b. In view of his/her specialist knowledge it is assumed that the user is already aware of the criminal-justice relevance of computer crimes, dealing in graphic or written pornography, or stealing, altering or otherwise manipulating data or programs. This specialist knowledge also relates to the sensitive issue of the transfer of data which can infringe on the privacy or personal integrity of others, or which violates existing copyright laws or licenses based on these laws.
 - c. Unauthorised usage of the computer network as in the following cases:
 - i. Gaining unauthorised access to information and resources of other account users without permission of the EDPC. This includes also the unauthorized access to computers of other users via monitor control or remote desktop access. The access of lecturers to the computers in computer rooms and laboratories during the lectures and exercises is allowed.
 - ii. Destruction of data and programs, i.e. the falsification and/or destruction of information of other users, especially through the infection of computer viruses.
 - iii. Obstruction of the network, i.e. technical disturbance of network operations or of other network users, e.g. by unsecured experiments in the network; attempts to crack passwords or by unannounced and/or unreasonable excessive burdening of the network to the disadvantage of other users or third parties.

- iv. It is forbidden to use P2P programs and file-sharing protocols within the HFT network. If such study supports are necessary, written authorization by the student's mentor is required.
- 8. You may only use those programs which have already been installed in the PC-pool rooms. It is forbidden for users to install their own programs.
- 9. A virus scanner with up to date virus signatures is mandatory for the use of private computers in the HFT network. The EDPC provides all members of the HFT with virus scanners for the most important software systems.
- 10. The EDPC reserves the right to check outgoing emails automatically for virus and other malware and to interrupt the delivery when indicated.
- 11. Violation of the above-mentioned points will result in your exclusion from access to the computer network.
- 12. The EDPC is authorised in the case of a functional failure, or whenever there is suspicion of misuse, to examine all of the data that can be found on a user's account.
- 13. In addition to the above-mentioned points, the operations and user regulations of the EDPC are also in force.
- 14. The EDPC give no warranty that its services are always available and error-free. There is also no warranty for correct and real-time email delivery.
- 15. Following exmatriculation from the student register accounts will be terminated and all account data will be deleted. Account termination takes place for teaching associates upon completion of their contract, for students upon exmatriculation and for employees upon termination of their contract at the HFT.
- 16. The user can increase the value of their printing allocation using the payment function on their student ID. If the printer that is charged using the printing allocation fails to work, the affected pages are then credited back to the allocation. The prerequisite for this is that the user submits the affected pages to the computer centre by no later than the next working day. Paid-for but unused pages can be paid back to the user at the end of their degree.
- 17. **Non-liability:** The computer centre is not liable for:
 - a. Damages on private computers that occur within the Stuttgart University of Applied Sciences. This includes damages and consequential damages resulting from (possibly erroneous) advice or support provided by staff or by installation and configuration of software provided by the EDPC. In particular, the EDPC is not liable for the deletion or modification of files and system settings, or for viruses, trojans, worms or other malware that can infect a private computer. Furthermore, the EDPC is not liable for typing errors made by employees, hardware damages, or the theft or destruction of data and software, in particular resulting from "infection" with computer viruses.
 - b. Tangible and intangible damages on private computers connected to the university network resulting from access to public resources (e.g. shared volumes). Examples of this include: Infection with computer viruses and spying on or destruction of private data.

Please fill in (readable in block-letters):

Matriculation number (Students only): _____	
Family name: _____	Given name: _____
Date: _____	Signature: _____