User Regulations for Networked Services provided by the Information Center at HFT Stuttgart

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 Informationszentrum (IZ = information center), IT-Support 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 IZ.

      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 IZ provides all members of the HFT with virus scanners for the most important software systems.

10. Violation of the above-mentioned points will result in your exclusion from access to the computer network.

11. The IZ 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.

12. In addition to the above-mentioned points, the operations and user regulations of the IZ are also in force.

13. The IZ give no warranty that its services are always available and error-free. There is also no warranty for correct and real-time email delivery.

14. 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.

15. 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 IZ by no later than the next working day. If a user ends their studies with credit on their print account after the deduction of the print allowance given to them by HFT Stuttgart they can have that credit paid out once their studies have officially ended.

16. **Non-liability:** The information center is not liable for:
   a. Damage caused to private digital devices within the HFT Stuttgart network. 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 IZ. In particular, the IZ 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 IZ 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. Material and immaterial damage may occur as a result of accessing open resources (e.g. shared directories) on private digital devices connected to the university network. Examples include infection with computer viruses and the phishing or deletion of private data.