Regulations for Use of the Information Processing Systems of the Bremen University of Applied Sciences

On October 12, 1998, the academic senate of the University of Applied Sciences of Bremen adopted the following regulations for the use of the information processing systems of the University of Applied Sciences of Bremen.

Preamble

The Bremen University of Applied Sciences (UAS Bremen) and its institutions ("operator" or "system operator") operate an information processing infrastructure (IP infrastructure) consisting of data processing equipment (computers), communication systems (networks) and further auxiliary IP facilities. The IP infrastructure is integrated in the German scientific network and accordingly in the world-wide Internet.

The regulations for use specified below regulate the conditions under which the IP services can be used.

§1 Ambit

These regulations apply to the IP infrastructure provided by UAS Bremen and its institutions.

§2 User Category and Responsibilities

(1) The operator's IP infrastructure is at the disposal of the members of UAS Bremen and beneficiary institutes of UAS Bremen for the fulfilment of their responsibilities in the areas of research, teaching, administration, training and further training, public relations work and publicity as well as other responsibilities described in the Bremen Higher Education Act.
(2) Other persons and institutions may be granted permission to use the system.

§3 Formal Authorization for Use

(1) The prerequisite for the use of the operator's IP resources is the formal authorization for use, to be applied for from the responsible system operator. Services provided for anonymous access (e.g. information services, library services, temporary guest ID codes for conferences) are exempt from this prerequisite.

(2) The system operator
- for central systems is the computer center (CC);
- for decentralized systems is the respective responsible organizational unit (department, institute, operational unit or other organizational unit of UAS Bremen)

(3) The application for formal authorization for use shall contain the following information:

- operator/institute or organizational unit from which the authorization for use is being applied for,
- the facilities for which the authorization for use is being applied for,
- applicant: name, address, telephone number, student registration number where applicable, affiliation with an organizational unit of the UAS Bremen where applicable,
- estimated purpose of use (e.g. research, training/teaching, administration),
- declaration of consent to comply with entries for the UAS Bremen information services (e.g. X.500),
- declaration of user's recognition of the Regulations for Use and of his/her consent to the acquisition and processing of personal data.

The system operator may request further information only to the extent necessary for the approval of the application.

(4) The responsible system operator decides on the approval/rejection of the application. He may make the granting of authorization for use contingent on proof of certain knowledge about the use of the system.

(5) The authorization for use can be denied if
- there is no apparent guarantee that the applicant will fulfil his obligations as a user;
- the capacity of the equipment whose use is being applied for does not suffice for the intended use due to the already existing rate of utilization;
- the applicant's intentions are not compatible with the purposes according to §2(1) and §4(1);
- the respective equipment is clearly unsuited to the intended mode of use or is reserved for special purposes;
- the equipment in question is connected to a network which must satisfy special data protection requirements and no substantive reason for the intended access is evident, or
- the use applied for will foreseeably disturb other authorized uses in an inappropriate manner.

(6) The authorization for use entitles the user to carry out work related to the use applied for only.

§4 Obligations of User

(1) The operator's IP resources may be used for the purposes specified in §2(1) only. Utilization for other purposes, particularly those of a commercial nature, can only be permitted upon application and against payment.

(2) The user is obligated to use the existing operation facilities (workplaces, CPU capacity, hard disk space, data line capacity, peripheral equipment and expendable material) in a responsible and economically sensible manner and to follow the instructions of the operator's personnel. In particular, the user is obligated to refrain from any action that causes impairments to the operation to the extent that such impairments are foreseeable and, to the best of his/her knowledge, to avoid any action which can cause damage to the IP infrastructure or other users. The user shall report any malfunctions of the system to the system operator immediately.

(3) The user shall refrain from all abusive use of the IP infrastructure. In particular, he/she is obligated
- to protect access to the IP resources by third parties by using a confidential password or corresponding method;
- to work exclusively with user codes which he/she has been granted permission to use;
- to take precautions to prevent unauthorized access to the IP resources; in particular to avoid the use of simple, easy-to-guess passwords, to change the passwords frequently and to carry out a logout upon completion of every work session. The user may not pass on any codes or passwords to third parties;
- to adhere to the legal regulations (copyright protection, etc.) in conjunction with the use of software (sources, objects), documentations and other data;
- to inform him/herself of the conditions under which the software – purchased in part within the framework of license agreements –, documentations or other data is placed at the user's disposal and to observe those conditions;
- in particular, unless by explicit permission, neither to copy, pass on or use the software, documentations and data for other than the authorized purposes, in particular not to use them for commercial purposes;
- to observe the user manuals placed at the user's disposal by the system operator;
- in the context of communication with the computers and networks of other operators, to observe the guidelines of the latter for use and access.

(4) Without the consent of the responsible system operator, the user may not
- interfere with the hardware installation in any way;
- change the configuration of the operating systems or the network.

The authorization to install software is regulated in conjunction with the respective local and technical circumstances.

§5 Data Protection

The user is obligated to coordinate any intentions to process personal data with the system operator before beginning. The provisions of the Data Protection Act are to be observed in any case.

§6 Responsibilities, Rights and Duties of the System Operator

(1) The system operator keeps an ongoing record of the authorizations for use which have been granted. The related documents are to be kept for two years following the expiration of the authorization.

(2) The system operator informs the users of the identity of the contact person charged with attending to the users.

(3) In an appropriate manner, in particular by taking regular samples, the system operator contributes to the prevention / exposure of abuse.

(4) The system operator is entitled

- to check the security of the system and passwords regularly with suitable software tools in order to protect his resources and the users' data from interference / damage by third parties;
- to document the activities of the user (e.g. by means of login times or connection data in network traffic) and evaluate the data collected if his doing so serves the purposes of accounting, resource planning, operation monitoring or the observation of errors and violations against the Regulations for Use and the legal provisions;
- in the presence of two persons and in compliance with the obligation to keep records, to inspect user files providing there is a specific basis for the assumption that the user has violated the Regulations for Use or committed a criminal offence, or providing such inspection is necessary to ensure proper operation;
- to employ measures to secure evidence if a suspicion of criminal offence has been corroborated.

(5) The system operator is obligated to treat information in due confidence.

(6) In the context of communication with the computers and networks of other operators, the system operator is obligated to observe the guidelines of the latter for use and access.

§7 System Operator's Liability / Exemption from Liability

(1) The system operator must furnish no guaranty that the system's functions will correspond to the user's special requirements or that the system will operate without defects or interruption. The system operator cannot guarantee the intactness and confidentiality of the data stored in his system.

(2) The system operator is not liable for damages of any kind resulting from the user's utilization of the IP resources unless provided for imperatively by legal stipulations.

§8 Consequences of Abuse or Illegal Use

(1) In the case of violation of legal provisions or of the provisions of these Regulations for Use, in particular of § 4 (Obligations of User), the system operator can limit or revoke the user's authorization for use.

(2) In the case of grave or repeated violations, a user can be permanently barred from the use of all IP resources of UAS Bremen.

(3) In the case of violations of legal provisions or of the provisions of these Regulations for Use, UAS Bremen explicitly reserves the right to initiate legal proceedings and pursue civil liability claims.

§9 Other Regulations

(1) Fees for the use of IP resources can be fixed in separate regulations.

(2) Supplementary or divergent regulations for use can be fixed for certain systems if necessary.

Supplement to the Regulations for Use of the Information Processing System of the Bremen University of Applied Sciences

On October 7, 2002, the academic senate of the University of Applied Sciences of Bremen adopted the following Supplement to the Regulations for Use of the Information Processing System of the University of Applied Sciences of Bremen adopted on October 12, 1998.

The following regulations apply to the operation and use of radio networks.

1. Definition of Terms

On the basis of radio technology, a Wireless Local Area Network (WLAN) connects WLAN access points and computers equipped with WLAN interfaces (primarily notebooks with WLAN-PCMCIA cards). The WLAN is connected to the university network.

2. Ambit of the Regulations for Use of the Information Processing Systems

- The Regulations for Use of the Information Processing Systems of UAS Bremen apply to the operation and use of the WLAN without restriction.
- In addition WLAN-specific regulations also apply. These regulations result primarily from the special network security requirements made necessary by the ease with which WLAN can be accessed via the radio fields of the WLAN access points, and serve as a means of countering the danger of unauthorized use and abuse of the university network by way of WLAN.

3. Responsibility

- The operator of the WLAN is the computer center (CC). Partial aspects of the operation for local areas of the WLAN can be delegated to the DP personnel of other institutions provided those persons fulfil the necessary technical and qualificational prerequisites. The overall responsibility for the operation and the guaranty of the security of the WLAN remains with the CC.
- The installation/alteration of the WLAN, particularly the installation/alteration of the WLAN communications channels, the connection to the university network and measures for the guaranty of security is reserved for the CC.
- The CC informs users of changes in the operation of the WLAN by e-mail as far in advance as possible.

4. Security Measures

- In order to guarantee the security of the WLAN, the CC is authorized to take the necessary measures, e.g. introduce safer access methods. The CC is also authorized to undertake security measures on short notice, e.g. to change the data encipherment key.

5. Prerequisites and Pointers for the Use of the WLAN

- Use of the WLAN requires a valid account for the user at UAS Bremen. The users are obligated to observe the Regulations for Use of the Information Processing Systems of UAS Bremen. In particular, the use of the network is permissible for purposes within the framework of research, teaching and administration. Every form of abuse of network resources or violation of network security is prohibited.

- Because of the fact that the WLAN radio medium is used jointly and because the protection mechanisms are incapable of providing complete security, the abuse of the WLAN by means of listening in cannot be entirely precluded. To the extent that a user requires protection of his data above and beyond the measures undertaken by the operator, the user must carry out this protection himself through the use of suitable encipherment methods which offer protection throughout the path of communication from the WLAN client to the destination station in the LAN or in the Internet.

- Violations of the Regulations for Use of the Information Processing Systems of UAS Bremen and/or of this Supplement can result in partial or complete exclusion from the entire IT infrastructure of UAS Bremen.