IVS-BO

C Hellmich

2018-4-19

Regulations for the Use of the Information Processing Systems of the Hochschule Hannover - University of Applied Sciences and Arts (IVS-BO)

Official Gazette of the Hochschule Hannover - University of Applied Sciences and Arts (HsH), Hanover, 27.7.2005, Issue 2/2005 Regulations for the Use of the Information Processing Systems of the Hochschule Hannover - University of Applied Sciences and Arts (IVS-BO) Issued by: The President of the Hochschule Hannover - University of Applied Sciences and Arts, Editors: President's Office and Press, Ricklinger Stadtweg 118, 30459 Hanover Tel.: 0511/9296-1013, Email: praesidialbuero@fh- hannover.de

At its 195th meeting on 5.7.2005, the Senate of the Hochschule Hannover - University of Applied Sciences and Arts (HsH) passed the following regulations for the use of the information processing systems of the HsH:

Preamble

These regulations for use are intended to ensure that the communication and data processing infrastructure of the HsH can be used as smoothly, unhindered and securely as possible. The regulations for use are based on the legally defined tasks of the HsH as well as on its mandate to safeguard academic freedom. They establish basic rules for the proper operation of the information processing infrastructure (IT infrastructure) and thus regulate the user relationship between the individual authorised users and the system-operating institutions of the HsH.

§ 1 Scope of application

These regulations for use apply to the use of the HsH's IT infrastructure, consisting of the data processing systems, communication systems and other facilities (including multimedia systems) for computer-based information processing.

§ 2 System-operating institutions

(1) System-operating institutions are those institutions which operate and administer an IT system which is part of the IT infrastructure.

(2) System-operating institutions include the computer centre as operator of the university network and the central systems and services of the HsH (central system operator) as well as the individual departments for their decentralised IT systems (decentralised system operators).

(3) The operation and support of the decentralised IV systems is carried out in agreement with the computer centre.

§ 3 Tasks of the computer centre

(1) The computer centre is responsible for the following tasks in particular:

1. Planning, realisation and operation of the IT infrastructure of the HsH for tasks in research, teaching, studies and administration,
2. Operational supervision of all IT systems in the HsH,
3. Coordinating the procurement of IT systems and standard software in the HsH, in particular

a) Opinions on investment measures in IT systems as well as
b) Utilisation analyses of existing system components and requirements planning,

4. Procurement, administration, documentation, maintenance of standard and basic software, in particular campus licences, as well as selection, use and support of the application software used in the university administration,
5. Instructions, consultation and support to users,
6. Support in the implementation of training and further education measures for members and staff of the HsH.

(2) The computer centre is also responsible for planning, installing and operating computer-based information and communication networks, including the necessary networks, central servers and data communication and telecommunication systems. In this regard, the computer centre is responsible for the following tasks in particular:

1. Provision and maintenance of a trouble-free and, as far as possible, uninterrupted operation of the communication network,
2. Coordinating the expansion and maintenance of the communications network,
3. Administration of the address and namespaces,
4. Provision of network services and central servers,
5. Supporting the authorised users in the use of the services.

(3) To ensure proper operation of the information and communication network as well as the IT systems assigned to the data centre, the head of the data centre may issue further rules for the use of the IT systems of the data centre, such as terms of use for the use of CIP pools and technical-organisational specifications for the operation of the data network.

§ 4 Usage rights and permission for usage

(1) All organisational units of the HsH are entitled to use the IT infrastructure.

(2) The following may be authorised to use the services of the system-operating institutions:

1. Members and affiliates of the HsH,
2. Authorised persons of the HsH for the fulfilment of their official duties,
3. Members and associates of other universities on the basis of special agreements,
4. Other state research and educational institutions and authorities of the state of Lower Saxony on the basis of special agreements,
5. Other institutions/persons associated with the HsH on the basis of special agreements or approvals, and
6. External public institutions or companies on the basis of special agreements or approvals.

(3) Approval is granted exclusively for scientific purposes in research, teaching and studies, for purposes of the library and the administration of the HsH, training and continuing education as well as for the fulfilment of other tasks of the HsH. Any use deviating from this shall be tolerated if it is minor and does not impair the purpose of the system-operating institutions or the interests of the other authorised users.

(4) Approval to use the IT infrastructure is granted by issuing a user authorisation and assigning a user ID. This is usually issued by the system-operating institution at the request of the authorised users. Excepted are services that are set up for anonymous access (e.g. information services, library services, short-term guest IDs for conferences).

(5) The application must contain the following information:

1. Name, address and signature of the applicant, as well as his or her status as per § 16, Paragraph 2 of the NHG, or other authorised user(s) as defined in § 4, Paragraph 2,
2. If applicable, description of the purpose of use or the planned project,
3. If applicable, desired IT resources
4. Acceptance of these regulations for use as well as the operating regulations issued pursuant to § 3, Paragraph 3 as the basis of the usage relationship,
5. Declaration of consent of the authorised user(s) to the processing of the personal data mentioned under points 1 to 3,
6. The authorised user's reference to the limited possibilities of documenting the user's behaviour and of inspecting the user files in accordance with § 7. Further information may only be collected if this is necessary for the decision on the application for approval.

(6) The authorisation to use the system is limited to the project applied for and may be limited in time. The system-operating institution may also provide approval for usage dependent on the proof of certain knowledge of the use of the desired IT systems and services.

(7) To ensure proper and trouble-free operation, the authorisation to use may be linked to a limitation of computing and online time as well as to other use-related conditions and requirements.

(8) If the capacities of the IT resources are not sufficient to meet the needs of all authorised users, the operating resources for the individual authorised users may be contingent by the system-operating institution, since the authorisation can only be granted within the limits of the available capacities.

(9) The authorisation of use shall be denied, revoked or subsequently restricted in whole or in part, in particular if

1. The preconditions for proper use of the IT infrastructure are not or no longer met,
2. The authorised user has been excluded from use in accordance with § 6,
3. The project of the authorised users is not compatible with the tasks of the system-operating institution and the tasks or purposes of the HsH,
4. The existing IT infrastructure is unsuitable for the use applied for or is reserved for special purposes,
5. The capacity of the IT infrastructure the use of which is requested is not sufficient for the planned use due to an already existing capacity utilisation,
6. The IT infrastructure to be used is connected to a network which must meet special data protection requirements and no objective reason for the planned use is apparent,
7. It is to be expected that the requested use will unreasonably interfere with other legitimate projects, or
8. In the case of institutions outside the universities, no proper application has been submitted or the information in the application is not or is no longer correct.

§ 5 Rights and duties of authorised users

(1) The authorised users have the right to use the IT systems of the system-operating institution within the scope of the authorisation and in accordance with these regulations for use.

(2) The authorised users are obliged

1. to observe the provisions of the Regulations for Use, in particular the purpose of use, and to comply with the limits of the usage right,
2. to refrain from anything that interferes with the proper operation of the IT systems of the system-operating institutions,

3. to treat all IT systems and other equipment of the system-operating institutions with care and consideration,
4. to work exclusively with the user IDs whose use they have been authorised to use within the scope of the licence,
5. to ensure that no other persons gain knowledge of the passwords of the users and to take precautions to prevent unauthorised persons from gaining access to the IT resources of the system-operating institutions. This includes protecting access by means of a password that must be kept secret and suitable, i.e. not easy to guess, and which should be changed as regularly as possible,
6. not to find out or use other people's user IDs and passwords,
7. not to gain unauthorised access to information of other authorised users and not to pass on, use or change information of other authorised users without permission,
8. when using software, documentation and other data, to comply with the statutory provisions, in particular those relating to copyright protection, and to observe the licence conditions under which software, documentation and data are made available by the system-operating institutions,
9. not to copy or pass on to third parties software, documentation and data provided by the system-operating institutions, unless this is expressly permitted, nor to use them for purposes other than those permitted,
10. to follow the instructions of the responsible personnel and to observe the respective room regulations,
11. not to remedy malfunctions, damage and errors in the IT equipment and data carriers of the system-operating institutions themselves, but to report them immediately to the responsible staff,
12. not to interfere with the installation and not to change the configuration of the IT infrastructure (including system-relevant user files) without the express consent of the system-operating institutions,
13. to provide the system-operating institutions with information on programs and methods used for control purposes and to grant access to the programs in justified individual cases, in particular in the event of justified suspicion of misuse and for troubleshooting,
14. to coordinate the processing of personal data with the system-operating institutions and, without prejudice to the authorised user's own obligations under data protection law, to take into account the proposed data protection and data security precautions.

(3) Authorised users shall use IT systems in a legally correct manner. In particular

the following behaviours are punishable:

1. Exploring other people's passwords, spying on data (§ 202 a of the StGB (German Penal Code)),
2. Unauthorised alteration, deletion, suppression or rendering unusable of data (§303a of the StGB),
3. Computer sabotage (§ 303 b StGB) and computer fraud (263 a of the StGB),
4. Dissemination of propaganda material of unconstitutional organisations (§ 86 of the StGB) or racist ideas (§ 130 of the StGB),
5. Dissemination of pornographic images (§ 184 of the StGB), in particular downloading or possession of child pornography (§ 184, Paragraph 5 of the StGB),
6. Offences of honour such as insult or defamation (§§ 185 ff of the StGB),
7. Criminal copyright infringements, e.g. by copying software in breach of copyright (§§ 106 ff of the UrhG (Copyright Act)).

§ 6 Exclusion from use

(1) Authorised users may be temporarily or permanently restricted in their use of the IT infrastructure or excluded from it if they

1. culpably violate these regulations for use, in particular the obligations listed in §5, or
2. misuse the IT infrastructure for criminal acts,
3. cause the HsH or third parties disadvantages or the risk of damage through other behaviour when using the IT infrastructure, or
4. damage the reputation of the HsH through the way it is used.

(2) Measures pursuant to paragraph 1 shall be taken only after a prior unsuccessful warning. The persons concerned shall be given the opportunity to comment. They may ask the chairperson of the senate commission for information technology to mediate. In the case of serious violations, a warning is not necessary.

(3) Temporary restrictions on use are to be lifted as soon as proper use is guaranteed again.

(4) A permanent restriction of use or the complete exclusion of an authorised user from further use shall only be considered in the case of serious or repeated violations within the meaning of paragraph 1, if proper conduct can no longer be expected in the future. The decision on a permanent exclusion shall be made by the university management after hearing the Senate Commission for Information Technology. Possible claims of the HsH arising from the user relationship remain unaffected.

§ 7 Rights and duties of the system-operating institutions

(1) The system-operating institutions shall keep a user file on the user authorisations granted, in which the user and mail identifications as well as the name and address of the authorised users are listed.

(2) Insofar as this is necessary for troubleshooting, system administration and expansion or for reasons of system security and protection of the usage data, the system-operating institutions may temporarily restrict the use of their IT infrastructure or temporarily block individual user IDs. If possible, the authorised users concerned must be informed of this in advance.

(3) If there are indications that authorised users make illegal content available for use on systems, the system-operating institutions may prevent further use until the legal situation has been adequately clarified.

(4) The system-operating institutions are entitled to check the security of the system/user passwords and the user data by regular manual or automated measures and to implement necessary protective measures, e.g. changes to easily guessed passwords, in order to protect the IT infrastructure and user data from unauthorised access by third parties. In the event of necessary changes to the user passwords, access authorisations to files and other protective measures relevant to use, the authorised users must be informed thereof without delay.

(5) In accordance with the following provisions, the system-operating institutions shall be entitled to document and evaluate the use of the IT systems by the individual authorised users in compliance with the data protection provisions, but only to the extent that this is absolutely necessary

1. to ensure proper system operation,
2. for resource planning and system administration
3. to protect the personal data of other authorised users,
4. for accounting purposes,
5. for the detection and elimination of faults, and
6. for the clarification and prevention of illegal or improper use.

(6) Under the conditions of paragraph 5, the system-operating institutions shall also be entitled to inspect the user files in compliance with data protection, insofar as this is necessary for the elimination of current faults or for the clarification and elimination of misuse and there are factual indications of misuse.

However, inspection of the message and email mailboxes is only permissible insofar as this is indispensable to rectify current faults in the message service. In any case, the inspection must be

documented and the data protection officer must be informed. The authorised users concerned shall be informed immediately as soon as this is possible without jeopardising the purpose of the measure.

(7) Under the conditions of paragraph 5, the connection and usage data in communications (in particular mail and telephone usage) may also be documented. However, only the detailed circumstances of the telecommunication - but not the non-public contents of the communication - may be collected, processed and used. The connection and usage data of the online activities on the Internet and other teleservices which the system-operating institutions make available for use or to which they provide access for use shall be deleted as soon as possible, at the latest immediately at the end of the respective use, insofar as this is not the billing data.

(8) In accordance with the statutory provisions, the system-operating institutions are obliged to maintain telecommunications secrecy and data protection.

§ 8 Liability of the authorised users

(1) The authorised users are liable for all disadvantages incurred by the HsH due to misuse or illegal use of the IT infrastructure. Furthermore, they shall be liable for disadvantages caused by the respective authorised users culpably failing to comply with their obligations under these Regulations for use. The liability regulations under labour and civil service law shall apply.

(2) The authorised users shall also be liable for damage caused by third party use within the scope of the access and use options made available to them if they are responsible for this third party use, in particular in the case of passing on a user ID to third parties. In this case, the HsH may demand a user fee for third-party use from the authorised users in accordance with the schedule of fees. In the event of such third-party use which has not been expressly approved, the institutions operating the system may exclude the authorised users from use in accordance with § 6.

(3) The authorised users shall indemnify HsH against all claims if HsH is held liable by third parties for damages, injunctive relief or in any other way due to abusive or illegal behaviour by the authorised users. The HsH will notify the authorised users of the dispute if third parties take legal action against the institutions operating the system.

§ 9 Liability of the HsH

(1) The HsH does not assume any guarantee or liability that the systems of the IT infrastructure will work without errors and at any time without interruption. Possible loss of data as a result of technical faults and the disclosure of confidential data by unauthorised access by third parties cannot be ruled out.

(2) The HsH does not accept any responsibility for the correctness of the programs made available. The HsH is also not liable for the content, in particular for the correctness, completeness and up-to-dateness of the information to which it merely provides access for use.

(3) In all other respects, the HsH is liable in relation to the authorised users only in cases of intent and gross negligence.

(4) Possible official liability claims against the HsH remain unaffected by the above regulations.

§ 10 Entry into force

These regulations for use shall enter into force on the day after their publication in the promulgating document of the HsH. At the same time, the user regulations for the data network and the connected data processing systems of the HsH of 28.01.1997 shall expire. Resolution of the Senate: 5.7.2005 Promulgating document: 2/2005 dated 27.7.2005