23 September 2008

UniReport

Goethe-Universität | Frankfurt am Main — Satzungen und Ordnungen

General Policy of Use for the ICT Infrastructure of the Johann Wolfgang Goethe University Frankfurt am Main (General ICT Policy of Use) as effective on 5 June 2001 and as amended on 11 September 2008

Preamble

The University and its departments and facilities are operating a computer aided information processing and communications infrastructure (ICT Infrastructure) consisting of information processing systems (computer systems) and a multi-service communications network for the transmission of voice, data and images. The ICT Infrastructure is integrated into the worldwide internet.

This Policy of Use governs the terms and conditions for the use of the services that are offered within this infrastructure;

- It is based on the statutory tasks of the University and its mandate to preserve the academic freedom;
- It provides the fundamental set of principles for the proper operation of the ICT Infrastructure;
- It refers to third parties' rights that have to be preserved (e.g. software licenses, compliance requirements of the network operators, data protection requirements);
- It obliges the user to act in an appropriate manner and to use the provided resources in an economical way; it obliges the providers to operate the system correctly;
- It informs on possible consequences arising from the violation of this Policy of Use.

The details relating to user registration and the operation of the computers are contained in the applicable Policy of Use of the individual organizational units.

§ 1 Scope of Application

This Policy of Use covers the ICT Infrastructure provided by the University; this infrastructure consists of facilities, data processing systems, information and communication systems and other support resources.

§ 2 User Groups and Purpose

1. The ICT resources listed in Article 1 are available to the members and associates of the University enabling them to fulfill their tasks in the fields of teaching, supply of information, administration, public relations as well as in the areas of education, training and further development of the University. Usage for other purposes than those listed above may be approved if the activities are not substantial and do not affect the interests of other users.

2. Students of the Johann Wolfgang Goethe University Frankfurt am Main are granted free use of the data processing facilities of the University upon matriculation. They should activate their access code immediately and check their e-mail account on a regular basis and/or redirect their e-mails to another account.

3. Staff members of institutions fulfilling the requirements of Article 3 (8) of the Universities Act of the Land Hesse (HHG) and staff of the Office of Student Activities (Studentenwerk) of Frankfurt am Main have the same status as user the groups defined in Fig. 1 of this Article.

4. Other legal entities and/or natural persons may be allowed to use the ICT Infrastructure upon application if third parties' rights remain unaffected.

§ 3 System Operator

1. System operator shall be the facility that operates and administers a data processing system that is part of the ICT Infrastructure.

2. The system operator for the University network and for the central systems and services is the University Computer Center (HRZ); for decentralized systems, this function shall be fulfilled by an organizational unit of the University (faculty, institute, work group, facility or any other subdivision of the University).

§ 4 Admission

1. To use the ICT resources in accordance with Article 1, the user must have a formal authorization issued by the responsible system operator (e.g. a user ID, network connection or network access authorized by the system operator).

2. The use of computerized services (e.g.: details of e-mail addresses, internet access, extensive computing time or storage capacity, use of PC pools) are governed by the policy of use issued by each organizational unity of the University.

3. Only members of the university (professors, staff members) may request the connection of computers to the university network; this request has to be submitted to their data processing coordinator and/or their domain administrator. The data processing coordinator and/or their domain administrator will inform on the rights and obligations and will record the relevant data to be forwarded to the University

Computer Center (HRZ). Computers that are operated by other members of the university and/or third parties may not be connected unless this has been authorized on the basis of special provisions and in cooperation with the University Computer Center (HRZ).

4. The University's general information systems (e.g. OPAC of the University's library system, www-server) may be used without user admission according to Fig. 1, if the responsible system operator has approved general access.

§ 5 Application for Admission

1. The application for admission has to contain the following information:
   a. The system operator who receives the application for admission;
   b. The system/systems for which admission is requested;
   c. The applicant's name, address, telephone number and/or fax number and e-mail address, if applicable. Students have to provide their matriculation number.
   d. Description of the intended use and/or the planned activities (e.g. research, teaching, supply of information, administration);
   e. Data protection statement for the processing of personal data by the applicant;
   f. Statement of acceptance made by the applicant that he or she accepts this Policy of Use and the Schedule of Fees of the University Computer Center (HRZ); both statements have to be submitted together with the application;
   g. The applicant's statement of acceptance that he or she agrees to the processing of their personal data for the purpose of user administration and, in particular, according to Article 8, Paragraph 5, 6 and 7 of this Policy.
   h. Warning that the applicant's user activities and user files may be recorded on the basis of this Policy.

   The application may contain a note informing the applicant that he or she may give his or her voluntary consent to the storage of his or her data in the system operator's information systems (e.g. X.500). Additional information may not be requested unless it is necessary to facilitate the decision for or against admission.

2. The data collected, stored and processed according to Fig. 1 (user information) may only be collected, processed and used to the extent as they are necessary to make the ICT resources (services) available to the user or if they are required for billing for services used (billing data). The may not be used for other purposes, e.g. controlling performance and behavior.

3. The admission is limited to the intended activities, for which the application was made, and it may be subject to a time limit. If the data processing capacities (e.g. computing and online time) are not sufficient to cover the overall user population needs, individual user resources may be restricted and/or tied to additional conditions and restrictions.

4. The admission for use is subject to the system operator's decision; prior to admission, the system operator may request the proof of certain skills how to use of the DP systems and DP services.

5. Admission may be rejected, withdrawn or retroactively limited in part or as a whole, in particular when
   a. no acceptable application has been submitted or when the information given in the application is incorrect or obsolete;
   b. when the requirements qualifying for adequate use of the DP facilities no longer exist;
   c. the applicant has been excluded from admission according to Article 7 Paragraph 1;
   d. the applicant's intended activities are incompatible with the tasks of the system operator and with the purposes listed in Article 2 Paragraph 1;
   e. the existing DP resources are reserved for special purposes or inadequate for the activities for which an application was made;
   f. the current levels of use exceed the capacities required for the intended use;
   g. the required EP components are connected to a network that has to meet special data protection requirements and there is no obvious need for the intended use;
   h. the purpose of use will potentially impair other authorized projects in an inacceptable way.

§ 6 Privileges and Responsibilities of Users

1. Upon admission the users are entitled to use the ICT Infrastructure as approved and as permitted by this policy and by other regulations. Any usage other than permitted by these regulations and policies requires special approval.

2. Central systems and services of the University Computer Center (HRZ) may be used by all members and associates of the University, decentralized systems may generally only be used by the members and associates of each organizational unit.

3. The users must comply with the provisions of these regulations and have to act within the boundaries of their admission, this applies in particular to activities according to Article 2 Paragraph 1;
   a. They are required to refrain from all activities that will disrupt the proper operation of the ICT Infrastructure;
   b. Wireless networks (Wireless LAN/WLAN) may be used within the IP network of the Johann Wolfgang Goethe University (141.2.0.0/16) only if they are used within the virtual local networks (VLAN) as provided by the University Computer Center (HRZ);
   c. They are required to handle all data processing systems, information and communication systems, as well as other resources of the ICT Infrastructure with due care; to use only the user codes that were permitted together with their admission;
   d. To take due care that their user passwords and user IDs are not made known to others and to make sure, when they use any resources within the ICT Infrastructure, that these resources cannot be accessed by unauthorized individuals; this includes the protection of the access with a strong password (difficult to guess) that must be

kept confidential and that should be changed on a regular basis;

e. Not to gain knowledge of or make use of other individual's user IDs;

f. Not to access information, and in particular, not to access other individual's messages without their authorization and not to pass on, use or modify any information gained on others without their approval;

g. When using software (sources, objects), documentation material and other data, the user must adhere to the legal provisions (e.g. copyrights) and comply with the contractual provisions (e.g. license agreements) under which the system operator provides purchased software, documentation material or data; in particular, not to copy software, documentation material and data, or to pass them on to third parties or to use them for purposes other than those permitted – this applies especially to commercial purposes – unless explicit permission has been given;

h. When providing www-information, to obey the policy for the internet presentation of the Johann Wolfgang Goethe University Frankfurt am Main, and to provide a declaration of responsibility (legal notice) on each www-page;

i. To follow the directions of the staff in all rooms of the system operator and to obey the University's and the system operator's house rules;

j. To produce the user admission on request;

k. Not to correct, mend or rectify problems, damage and errors of DP resources and data media but to immediately report them to the responsible staff member;

l. Not to make changes to hardware installations and/or to the configuration of the operating systems, system files, and user files that are required by the system, and to the network, unless explicit approval has been obtained; the privileges to install software are governed by a separate policy and they depend on the local system technologies;

m. When requested by the responsible system operator, and especially when possible abuse has to be suspected, to give the system operator access to information on programs and methods used, to enable the system operator to undertake troubleshooting and controls, and to grant the system operator access to the programs and files, unless these are protected pursuant to the secrecy of telecommunication, confidentiality of data and/or similar regulations, e.g. personal files or data of third parties;

n. To cooperate with the data protection officer of the University and with the responsible system operator when personal data have to be processed, taking into account the data protection proposals and data security proposals made by the system operator and observing all personal data protection obligations that may exist.

4. Please note that especially the following offences and/or crimes are subject to punishment:

   a. Data espionage (German German Penal Code (StGB), Section 202a),
   b. Data manipulation (German German Penal Code (StGB), Section 303a),
   c. Computer sabotage (German German Penal Code (StGB), Section 303b),
   d. Computer fraud (German German Penal Code (StGB), Section 263a),
   e. Dissemination of pornographic publications (German German Penal Code (StGB), Section 184), especially downloading or possessing child pornographic material (German German Penal Code (StGB), Section 184 Paragraph 5),
   f. Dissemination of propaganda material of unconstitutional organizations (German German Penal Code (StGB), Section 86) and sedition (German German Penal Code (StGB), Section 130),
   g. Defamation, such as libel or slander (German Penal Code (StGB), Sections 185 et seq.),
   h. Reviling or abusive speech or remarks on creeds, religions and/or beliefs (German Penal Code (StGB), Section 166),
   i. Punishable copyright violations, e.g. by the illegal reproduction of software or entering protected works into a DP system (German Copyright Law (UrhG), Section 106 et seq.).

5. The users and the system operators must keep up to date with the relevant provisions, especially with the provisions contained in the Data Protection Law of the Land of Hesse (Hessisches Datenschutzgesetz).

§ 7 Exclusion from Use

1. Users may temporarily or permanently be limited in or excluded from the use of the DP resources

   a. if they intentionally or negligently violate this Policy and, in particular, the obligations listed in Article 6 (abusive actions) or

   b. when they abuse the DP resources for illegal/criminal acts

   c. or when they cause harm to the University by other unlawful user behavior.

2. Actions according to Article 1 shall only be taken when warning notices have failed to produce any effect. The person concerned shall have the opportunity to present comments.

3. Temporary usage restrictions that will be implemented by the responsible system operator have to be lifted as soon as compliant use can be expected.

4. A permanent restriction or revocation of user rights is only possible in cases of severe and repeated violations pursuant to Article 1, and when compliance cannot be expected in the future, although actions have already been taken. The decision to permanently remove the privileges to use a system operator's system shall be made by presidential notice upon application of the system operator. All claims of the University and of the system operator that may arise from the usage relationship shall

remain unaffected.

§ 8 Privileges and Responsibilities of the System Operator

1. Each system operator has to inform the users on the usage, important facts and the relevant rules and regulations to be obeyed, and in particular, on their privileges and responsibilities as stated in Article 6.

2. Each system operator may maintain a user file containing the personal data of the users. A summary of the type of data stored must be accessible to each user at any time.

3. Each system operator shall publish the names of the system administrators in charge of the system. Each system operator and each system administrator is bound by secrecy.

4. System operators offering the users the possibility to publish their own homepages in the Internet have the right to generate an automated legal notice containing the full name and the e-mail address of the author.

5. Each system operator has the right to limit the use of his or her resources for a certain time or to block individual user IDs, to the extent as is necessary for troubleshooting, system administration and system extension as well as for system security and for the protection of user data. If possible, the affected user has to be informed ahead of time.

6. To protect the DP resources and user data from unauthorized use by third parties the system operator may apply manual or automated check procedures on a regular basis to control the security of the system and /or user passwords and user data and may implement all necessary protective measures, e.g. changing passwords that can easily be guessed. All necessary changes of user passwords, access privileges to user files and other user-relevant protective measures have to be communicated to the user without delay.

7. On the basis of the laws as listed in the following, and on the basis of the provisions of this Policy of Use, each system operator has the right to document and evaluate how individual users use the data processing systems (operation, connection and usage data), if a necessity exists:

   a. to ensure the correct operation of the system,
   b. to plan resources and to administer the system,
   c. to protect the personal data of other users,
   d. for billing purposes,
   e. to identify and correct system troubles, and
   f. to detect and prevent abusive, or unlawful use.

8. Subject to Article 6, and subject to the adherence to secrecy, each system operator may access the user files, if deemed necessary, to clear existing system troubles or to detect and prevent abuse. Accessing messages and e-mail inboxes is only allowed if this is necessary to correct existing problems within communications service. This access requires the presence of another staff member. Any access has to be documented. The affected user has to be notified immediately when the purpose has been attained. If the investigation provides evidence for punishable offences/criminal acts, the Head of University has to report the incident to the Department of Public Prosecution.

9. Under the preconditions described in Paragraph 6, and if the investigation provides actual evidence that the user stores contents for general use on the servers of the University that violate the laws or the provisions contained in this Policy, the system operator has the right to block the contents for general access at any time. If the investigation provides actual evidence that a user processes illegal contents on the servers of the University, the system operator may also take measures to seize evidence in coordination with the Head of University and the competent authorities, if necessary.

10. Based on the provisions of Article 6, the connection and usage data within communication traffic (in particular within e-mail traffic) may also be documented. But only the specific circumstances of the telecommunication may be gathered, processed and used, not however, the non-public contents of the communication. When recording of the connection data of the www-usage (e.g. accessing the data stored on a www-server) no personal data may be documented.

11. To ensure the proper operation of the system, each system operator is entitled to check the e-mail traffic for malicious programs (e.g. virus) using an automated procedure. If the investigation provides actual evidence that an e-mail contains a malicious program, it may be automatically deleted; the sender and the receiver have to be informed.

12. To ensure the proper operation of the system, each system operator is entitled to check the e-mail traffic for annoying mails (e.g. unsolicited bulk e-mails [SPAM]) using an automated procedure. If there is actual evidence that an e-mail contains abusive contents, the system operator has the right to add a warning to the email; but it has to be delivered without further changes. Users may object to this safety check and they will receive their e-mail unexamined.

13. All connection and usage data relating to online activities in the internet and other services that are offered or made accessible by a provider must be deleted as soon as possible, at the latest, however, at the end of each session, unless the data are required for operating or billing purposes.

14. The user data must be deleted by the system operator as soon as possible, at the latest, however, immediately at the end of each session, provided the data are not required for billing purposes.

15. Each system operator shall delete all data required for billing as soon as they are no longer necessary for billing purposes; user-related billing data required for the itemization of certain services must not be kept longer than 80 days after the bill has been sent out, unless the payment of the outstanding amount is challenged within this period or it has not been settled although a demand notice has been sent.

16. It is not permitted to communicate personal data or operating data, connection data and user data that enable the identification of individuals. The powers of the law enforcement authorities shall remain unaffected.

17. Pursuant to the relevant legal provisions, each system operator is obliged to ensure the telecommunications and data secrecy.

§ 9 User Liability

1. Each user shall be liable for all offers provided by him or her, especially for the contents of their www-pages;
2. The user shall be held liable for all disadvantages incurred by the University as a result of wrongful or illegal use of the DP resources and user admission or that arise as a result of the user's intentional or negligent violation this Policy.
3. The University may claim compensation for the wrongful use of resources and other costs pursuant to the Schedule of Fees, which have to be borne by the user. Further claims for compensation remain unaffected. The user shall also be held liable for damages caused by third parties, if the user is accountable for third parties using his or her access and user privileges; this applies in particular to third parties using his or her user ID. In this case, the University may charge user fees for the use by third parties pursuant to the Schedule of Fees. Any other claims for compensation shall remain unaffected.
4. The user shall to hold the University harmless of claims if third parties assert claims for compensation, injunctive reliefs or similar compensation as a result of the user's wrongful or unlawful use.

§ 10 System Operator's Liability / Exemption from Liability

1. The system operator does not guarantee that the system will run without errors and interruption at all times. Any loss of data as a result of technical problems and/or third parties gaining knowledge of confidential data through unauthorized access cannot be excluded. The respective system operator cannot accept any guarantee for the integrity (e.g. destruction, manipulation) and confidentiality of data stored on his or her resources.
2. The system operator assumes no responsibility for the correctness of the programs provided by him or her. The system operator shall not be made liable for the contents; he or she shall, in particular, not be held liable for the correctness, completeness and current relevance of information to which he or she provides the access only.
3. The system operator shall not be liable for damages of any kind that are incurred by the user as a result of using the ICT resources pursuant to Article 1 of this Policy, unless there are legal provisions that supersede this Policy.
4. Any claims against the University that may arise as a result of the so-called "liability of public authorities regulation" (Amtshaftungsansprüche) shall remain unaffected by the above provisions.

§ 11 Other Provisions

1. Charges or fees may be levied for the use of ICT resources. The Schedule of Fees of the relevant system operator shall be applicable.
2. All system operators shall supply within the given technical possibilities an alias as login name that allows no conclusions as to the user's name, sex, position and/or other characteristics.
3. In agreement with the other system operators the University Computer Center (HRZ) develops rules defining the details of their cooperation.
4. All system operators may stipulate supplementary or differing user rules, if necessary.
5. For the use of the infrastructure and the services provided by the University Computer Center (HRZ) fees and charges have to be paid as laid down in the HRZ Schedule of Fees (HRZ-Entgelteordnung). This HRZ Schedule of Fees (HRZ-Entgelteordnung) will be decreed by the Executive Board (Präsidium) on proposal of the University Computer Center (HRZ).

§ 12 Transition Provisions

The Policy of Use for the Information Processing systems (DP Infrastructure) of the University Computer Center (HRZ) of the Johann Wolfgang Goethe University Frankfurt am Main, dated 14 November 1996 and as amended on 24 April 1997, shall become ineffective.

§ 13 Effective Date

This Policy shall become effective upon the resolution of the Executive Board (Präsidium) on the day following its publication in UniReport Aktuell.

Frankfurt am Main, 23 September 2008

Prof. Dr. Wolf Assmus

Vice President

www.satzung.uni-frankfurt.de

Legal Notice

The UniReport is published as a special edition of the UniReport on an irregular basis and as the need arises. The number of copies will be determined individually for each issue.

Published by: Der Präsident der Johann Wolfgang Goethe-Universität Frankfurt am Main

---

I, the undersigned, a duly sworn and authorized translator for the English language for the Law Courts and Notaries in the State of Hesse, Federal Republic of Germany, hereby certify that the foregoing is a complete and true translation as made from the original certificate titled "Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikations-Infrastruktur der Johann WolfgangGoethe-Universität (Allgemeine IuK-Nutzungsordnung) vom 5. Juni 2001 in der Fassung vom 11. September 2008".

Frankfurt/Main, February 20, 2012

Martina Hohlrüther
Allgemein ermächtigte Übersetzerin in der englischen Sprache für die Gerichte und Notare im Land Hessen
Sworn and Authorized Translator for the Courts and Notaries of the State of Hesse
LG FFM 316 E - 46 -33

Digital unterschrieben von Martina Hohlrüther
DN: cn=Martina Hohlrüther, o=für die Gerichte und Notare im Land Hessen, LG Frankfurt/M., ou=Allgemein ermächtigte Übersetzerin in der englischen Sprache, email=mh.ffm@arcor.de, c=DE
Datum: 2012.02.19 19:17:32 +01'00'