Acceptable Use Policy
for Information Processing Systems
at the Catholic University of Eichstätt-Ingolstadt

Last updated: 1 March 2016

Preamble

The Catholic University of Eichstätt-Ingolstadt and its institutions (the "operators" or "system operators") operate an information processing infrastructure, consisting of data processing equipment (computers), communications systems (networks), and other support elements used for information processing. The information processing infrastructure is integrated into the German National Research and Education Network (Deutsches Wissenschaftsnetz; WiN) and the Internet.

This policy governs the conditions under which the information processing infrastructure and the accompanying services may be used.

This policy

- is based on the legal responsibilities of universities and their mandate to protect academic freedom;
- establishes basic rules to ensure the proper operation of the information processing infrastructure;
- indicates the rights of third parties which must be observed (e.g. software licenses, network provider requirements, data protection issues);
- requires the user to adhere to a proper code of conduct and to use the available resources efficiently;
- provides information about the operator's rights and remedies in the event of a violation of the acceptable use policy.

Section 1 Scope

(1) This acceptable use policy applies to the information processing infrastructure operated by the Catholic University of Eichstätt-Ingolstadt and its constituents, including data processing equipment (computers), communications systems (networks), and other support elements for information processing.

Section 2 Users and Functions

(1) Members of the Catholic University of Eichstätt-Ingolstadt are granted access to the information processing infrastructure mentioned in Section 1 in order to perform their functions in areas of research, teaching, university administration, central services, training, public relations and to fulfill other responsibilities specified in Art. 2 of the Bavarian Higher Education Act (Bayerisches Hochschulgesetz, BayHSchG).

(2) Additional persons and institutions may also be granted access.

(3) Members of the Catholic University of Eichstätt-Ingolstadt should contact either the University Data Center or the organizational unit responsible for them (see Section 3.1).

Section 3 Formal User Authorization

(1) Use of the information processing infrastructure as per Section 1 requires formal user authorization from the appropriate system operator. This rule does not apply to services which are designed for anonymous access (e.g. information services, library services, temporary accounts for conference guests).

(2) The system operators responsible for

a) centralized systems, decentralized servers as well as the university network is the University Data Center;

b) other decentralized systems are the organizational units of the university (faculties, institutes, operational divisions, chairs or departments, or other subunits).

(3) An application for formal user authorization should include the following information:

- The name of the operator/institute or organizational unit from which you are requesting authorization;
- The systems for which you are requesting user authorization;
- The applicant's personal information: Name, date of birth, address, telephone number, student registration number (if applicable), and home department or organizational unit at the university.
- General information on the intended use of the services, e.g. research, training/teaching, administration;
- A statement regarding acknowledgment of the acceptable use policy;
- Information required for data entries used by the information services of the university.

The system operator may only request further information if necessary to facilitate the decision to accept or decline an application.

(4) The system operator responsible decides over the acceptance or rejection of applications. The system operator may make the approval of an application dependent on proof of certain skills or knowledge regarding the use of the facilities.

(5) User authorization may be denied if

a) there is reason to believe that the applicant will not be able to fulfill their obligations as a user;

b) the capacity of the facility for which the user is requesting authorization is insufficient for the user's purposes because another request has already been authorized;

c) the proposed use is not in accordance with the purposes stipulated in Section 4.1;

d) the facilities are not suitable for the proposed use or are already reserved for special purposes;

e) the facilities in question are part of a network with special data protection requirements, but no practical reasons for the access request can be identified;

f) it appears that other users will be inordinately disturbed by the proposed use.

(6) The user authorization is only valid for tasks connected with the proposed use stated in the application.

Section 4 User Obligations

(1) You may use the information processing resources as described in Section 1 only for the purposes stipulated in Section 2.1. You must submit an additional application and payment for any other use, especially commercial use.

(2) Technical equipment and resources (workstations, CPU capacity, disk space, cable capacity, peripherals and other supplies) must be treated with care and used in an efficient and responsible manner. Users must refrain from actions that are likely to disrupt operations and, to the best of their knowledge, actions that might damage the information processing infrastructure or the work and property of other users.

Violations of this policy may result in damage claims (see Section 7).

(3) Users are to refrain from improper use of the information processing infrastructure. Users are additionally required to

a) use only accounts which they have express permission to use; it is prohibited to share login information with others;

b) protect access to information processing resources with a secret password or similar means;

c) take measures to prevent unauthorized third parties from gaining access to information processing resources; this means, for example, avoiding passwords that can be easily guessed, changing passwords frequently, and logging out at the end of every session.

Users assume full responsibility for all activities conducted via their account, including activities undertaken by third parties explicitly given access to the account or who gained access due to negligence on the user's part.

Users are furthermore required to,

a) observe regulations stipulated by law (e.g. intellectual property rights, copyright) when using software (source, object), documentation and other data;

b) inform themselves about and adhere to the conditions under which the software (part of which may have been acquired under license agreements), documentation, and data are provided;

c) refrain from copying or sharing software, documentation, or data without express permission, nor use said software for purposes other than those permitted, especially not for commercial purposes.

Violations of these rules may result in damage claims (see Section 7).

(4) Use of the information processing infrastructure obviously must adhere to the law and relevant legal regulations. It should be explicitly noted that the following acts are punishable under German law:

a) Attempting to capture passwords, intercepting data (Section 202a of the German Criminal Code (Strafgesetzbuch, StGB));

b) Changing, deleting, hiding, or destroying data without authorization (Section 303a StGB);

c) Computer sabotage (Section 303b StGB) and computer fraud (see Section 263a StGB);

d) Disseminating propaganda material from unconstitutional organizations (Section 86 StGB) or disseminating racist ideas (Section 131 StGB);

e) Distributing certain types of pornography on the Internet (Section 184.3 StGB);

f) downloading or being in possession of documents containing child pornography (Section 184.5 StGB);

g) defamation, libel, slander and the like (Section 185 and following StGB).

The Catholic University of Eichstätt-Ingolstadt reserves the right to initiate steps towards criminal proceedings and the right to make claims under civil law (see Section 7).

(5) Users must obtain permission from the system operator in order to

a) alter the hardware installation;

b) change settings to the operating systems or the network.

Software installation rights are regulated separately and depend on individual conditions as well as technical and system requirements.

(6) Users must communicate plans to edit personal data to the system operator before carrying out any changes. This policy does not affect any of the rules or requirements stipulated by data protection law.

Users are prohibited from reading or processing messages intended for other users.

(7) Users must

a) observe user guidelines as provided by the system operator;

b) uphold the acceptable use policies of other service providers when working with their computers and networks.

Section 5 Responsibilities, Rights and Obligations of System Operators

(1) All system operators shall keep a record of user authorizations. Records will be kept for at least two years following the expiration of the user's authorization.

(2) To prevent and detect improper use, system operators may act accordingly, for example by carrying out spot checks. In this respect, they are authorized to

a) document and assess user activity when necessary for billing purposes, resource planning, or system monitoring, and in order to check on malfunctions or violations against this policy or legal regulations;

b) access a user's files and e-mail accounts, and document in detail their use of the network (e.g. by using a network sniffer) if there are reasonable grounds to suspect violations against the acceptable use policy or criminal infractions; the two-person rule and record-keeping requirements must be observed;

c) implement measures (such as keystroke logging or network-sniffer) to secure evidence in instances where suspicions of criminal activity have been substantiated.

Any user who is subject to such investigatory measures as described in b) and c) must be informed about them once the operation has ended.

(3) The system operator is required to maintain confidentiality.

(4) The system operator provides information on the contact persons responsible for user support.

(5) The system operator must observe the acceptable use policies and access agreements of other service providers when working with their computers or networks.

Section 6 System Operator's Liability and Exemptions

(1) The system operator offers no guarantee that the system's functions will correspond to the specific requirements of the user or that the system will run without errors or interruptions. The system operator cannot guarantee the integrity (against threats of corruption or manipulation) or confidentiality of stored data within the system.

(2) The system operator and the Catholic University of Eichstätt-Ingolstadt are not liable for damages to users that result from their use of the information processing resources as described in Section 1; malicious activities committed by the system operator or anyone working for the system operator are not exempt from liability.

Section 7 Consequences of Improper or Criminal Use

(1) Violations of the law or the regulations included in this acceptable use policy may result in the system operator limiting or temporarily revoking user authorization until it is clear that that the user will henceforth refrain from improper use of the information processing resources. It is irrelevant in such cases whether the violation resulted in material damages.

(2) In cases of egregious or multiple violations, users can be permanently banned from using any and all information processing resources as described in Section 1.

(3) Violations of legal provisions or the regulations stipulated in this acceptable use policy will be weighed according to their relevance to criminal and/or civil prosecution. Significant cases will be passed along to the appropriate legal department, which then decides if further action is necessary. The Catholic University of Eichstätt-Ingolstadt reserves the right to initiate steps towards criminal proceedings as well as the right to seek legal remedy under civil law.

Section 8 Other Regulations

(1) Additional provisions may stipulate that fees for the use of information processing resources are required.

(2) Supplementary regulations may be issued for certain systems if required.

(3) The courts of Ingolstadt shall be the place of jurisdiction for legal claims arising from user activities.

Came into effect through senate approval on 24 July 1996; amended to conform with new university constitution approved by the senate on 6 February 2002.

In case of deviations between the German and the English version, the German version shall prevail.