Regulations for the IT Infrastructure at the University of Bayreuth 30 November 2018

On the basis of Art. 13 para 1 sentence 2 and Art. 25 para 3 no. 1 of the Bavarian Higher Education Act, the Senate of the University of Bayreuth enacts the following Regulations for the IT Infrastructure of the University of Bayreuth (IT Regulations).

Contents

Preamble

[1]The University of Bayreuth and its institutes have a data-processing infrastructure (IT infrastructure) comprising the various information processing units (computers, end devices with computer functionality and connectivity, and any physically or virtually networked objects), communications systems (networks), and other IT support facilities. [2]The IT infrastructure is integrated in Germany's scientific network and thus also in the internet worldwide.
[3]The guidelines presented here govern the use and operation of the IT infrastructure.
[4]These guidelines

- are based on the legally defined tasks of institutions of higher education and their mandate to ensure academic freedom
- provides ground rules for orderly use of the IT infrastructure
- indicate rights to be protected for third-parties (e.g. software licenses, network provider's terms, data protection issues)
- obligate the user to observe good conduct and make economical use of the resources offered
- provide information on measures available to the system administrator if the regulations are breached.

The University of Bayreuth is not liable for inaccuracies or mistakes in this English translation.
In case of doubt, the German originals are to be used in a court of law.

§1 Scope

(1) These guidelines apply to the IT infrastructure operated at the University of Bayreuth, which comprises information processing units (computers, end devices with computer functionality and connectivity, and any physically or virtually networked objects) communications systems (networks), and other IT support facilities.

(2) These guidelines can be amended by the system administrator through additional regulations according to §3(2), as long as they do not breach the terms of the present regulations.

§2 User group and assigned tasks

(1) The IT infrastructure referred to in §1 is available to members of the University of Bayreuth to support them in fulfilling their duties in research, teaching, administration, education, continuing education, public relations, presenting the University, as well as other duties mentioned in Article 2 of the Bavarian Higher Education Act.

(2) Other persons and institutes can be granted access by the President's Council if they submit an application in writing.

§3 Formal authorization for use

(1) Anyone who would like to use the IT infrastructure under §1 must first be granted a formal authorization for use by the relevant system administrator in accordance with §3(2).

(2) The system administrator

a) of the central computing systems and of the communications system (university data network) is the IT Service Centre and

b) of the peripheral computing systems is the relevant organizational unit (faculty, chair, or other sub-unit of the University of Bayreuth).

(3) [1]The application for formal authorization for use is to contain the following information:

- system administrator (organizational unit, e.g. chair or IT Service Centre), to whom the application is submitted
- systems for which authorization is requested
- applicant: name, address, telephone number, enrolment number (if applicant is a student), and any affiliation with an organizational unit of the University
- A general statement regarding the purpose of use, such as "research", "teaching/ education", or "administration"
- entries for the University's address book/ directory
- statement that the user accepts the terms of the present guidelines and consents to the collection and processing of his or her personal data under the terms of §5(4)

- if applicable, name and signature of the head of the organizational unit (e.g. chair).

[2]The system administrator may only request additional information to the extent that it is required in order to make a decision concerning the application.

(4) [1]The relevant system administrator under the terms of §3(2) shall make a decision concerning the application. [2]He may make authorization conditional on knowledge of how to use the computer equipment.

(5) Authorization may be refused if

a) there is doubt as to whether the user will fulfil his duties

b) the capacity of the system for which the application was submitted is insufficient for the planned activities due to current use

c) the planned activities are incompatible with §2(1) and §4(1)

d) the computer system is patently inappropriate for the planned activities or is reserved for special purposes

e) the computer system to be used is connected to a network that is subject to special data protection requirements, and the facts do not seem to justify this request for access

f) it is probable that the planned activities will disproportionately interfere with the activities of other authorized users.

(6) The authorization for use only applies to activities relating to the type of activity for which the application was submitted.

§4 User responsibilities

(1) The IT infrastructure as defined in §1 may only be used for the purposes mentioned in §2(1).

(2) [1]The user is required to ensure that the available equipment (work stations, CPU capacity, hard drive storage capacity, capacity of electric lines, supplies, and peripheral devices) is used responsibly and economically. [2]The user is required to abstain from causing interference to operations to the extent that this can be foreseen, and to avoid any activities which, to the best of his knowledge, could damage the infrastructure or the work of other users. [3]Damage claims may arise as a result of failure to comply (§7).

(3) [1]The user shall abstain from any improper use of the IT infrastructure. [2]In particular, he shall

a) abstain from working under a username for which he is not authorized; the sharing of usernames and passwords is prohibited

b) take precautions to ensure that unauthorized third parties do not gain access to the IT infrastructure; this includes avoiding simple or obvious passwords, changing your password frequently, and logging out.

[3]The user bears full responsibility for any activities that are carried out under his username; this also applies if negligence on the part of the user leads to access by the third parties.[4]In addition, the user is required

a) to observe the regulations for using software (sources, objects) as well as the documentation and any other legal regulations (copyright)

b) to inform himself of the terms and conditions – based in part on license agreements – for the software, documentation, or data, and to observe these regulations

c) particularly with regard to software, documentation, and data: to abstain from copying or distributing without express permission, especially for commercial purposes

d) to observe the laws and regulations concerning data protection as well as the regulations contained in the terms of use for websites visited

e) to strive for accessibility when creating content.

[5]Damage claims may arise as a result of failure to comply (§7).

(4) [1]It goes without saying that illegal use of the IT infrastructure is prohibited. [2]The following activities, which are punishable under the terms of the Criminal Code (*StGB*) are mentioned explicitly:

a) data spying (§202a *StGB*), intercepting data (§ 202b StGB), preparing for data spying or intercepting data (§ 202c StGB), or receiving stolen data (§ 202d StGB)

b) unauthorized changing, deleting or suppressing data, or rendering data useless (§303a StGB)

c) computer sabotage (§303b *StGB*) and computer fraud (§263a *StGB*)

d) spreading propaganda of unconstitutional organizations (§86 *StGB*) or racist ideologies (§130 *StGB*)

e) spreading certain types of pornography via the internet (§184 para 3 *StGB*)

f) accessing or possessing documents containing child pornography (§184 para 5 *StGB*)

g) offenses such as insult or defamation (§§185 ff *StGB*).

[3]The University of Bayreuth reserves the right to take legal action in the form of criminal as well as civil litigation (§7).

(5) [1]The user is prohibited from the following without the prior consent of the **relevant** system administrator:

a) carrying out hardware modifications;

b) changing the configuration of the operating systems or network.

[2]Rights concerning the installation of software depend on the circumstances of the region and the system and are thus addressed separately.

(6) [1]The user is obligated to clear any plan to process personal data with the system administrator. [2]The obligation to observe the regulations set forth in the Data Protection Act (*Datenschutzgesetz*) remains in force.

[3]The user is not permitted to read messages that were meant for others or to make use of such messages.

(7) The user is required to adhere to

a) the user guidelines provided by the system administrator

b) the user guidelines of other providers when using their computers and networks.

§5 Tasks, rights, and responsibilities of the system administrator

(1) [1]Each system administrator shall create the following for his or her systems in cooperation with those responsible for data protection and information security

a) the registers of processing activities relating to personal data, a risk analysis of the intended processing activities and, in the event that a high level of risk to data protection is expected, the data protection impact assessment;

b) the necessary data protection information;

c) the documentation of the protective measures and the necessary safety concepts, to the extent that they are required by law (in particular in accordance with BayEGovG, TKG, TMG, BayHO)

d) documentation of user authorizations.

[2]These documents are to be kept for at least six months following expiration of the authorization period.

(2) The system administrator shall publish the contact for user support.

(3) [1]The system administrator shall make a moderate contribution to preventing and exposing abuse or violation of these guidelines and especially against copyright, data protection, or criminal law. [2]For this reason, he or she is, in particular,

a) authorized to use appropriate tools to monitor the security of the IT infrastructure for which he or she is responsible, in particular, by way of random inspection, in order to protect his or her resources and the user's data from attacks carried out by third parties;

b) only authorized on suspicion of a user violating these guidelines or criminal law - in accordance with the four-eyes principle and the record-keeping requirement – to view that user's computer files or history;

c) is authorized, in the case of confirmed suspicion of punishable offenses, to take measures required to secure evidence if necessary.

(4) [1]The system operator shall be entitled to document and evaluate the activities of the users (e.g. through the login- and times or the connection data in the network) within his or her area of responsibility, subject to compliance with legal requirements. [2]Documentation and evaluation must be related to the purpose of accounting, uncovering the unlawful use of the system (provided that there are factual indications of such use), resource planning, as well as safeguarding operations, of breaches of these regulations or of legal regulations. [3]The data can also be processed, if necessary, to recognize, isolate, or eliminate malfunctions or errors.

(5) The system administrator shall undertake to treat information confidentially.

(6) The system administrator is obligated to adhere to the regulations of other providers when using their computers and networks.

(7) The system administrator can temporarily or permanently limit use of the IT resources in order to preserve IT security.

§6 Liability

(1) [1]The system administrator can guarantee neither that system functions will meet the special needs of the user nor that the system will work flawlessly and without interruption. [2]The system administrator cannot guarantee the integrity (with regard to destruction or manipulation) or confidentiality of saved data.

(2) The system administrator shall not be held liable for damages of any kind which the user may incur as a result of using the IT infrastructure in the sense of §1 unless other legal proceedings render this necessary.

§7 Consequences of misconduct or illegal use

(1) [1]If the user breaks the law or violates the terms of these guidelines, especially §4 (User responsibilities), the system administrator can limit or revoke authorization for use. [2]This is irrespective of whether or not material damages were incurred.

(2) A user can be permanently banned from the entire IT infrastructure in the sense of §1 in cases of serious or repeated violation.

(3) [1]Violations of the law or of the regulations set forth in these guidelines will be considered for criminal prosecution and civil proceedings. [2]Matters that appear relevant shall be forwarded to the legal department, which shall then consider the next steps to be taken. [3]The University of Bayreuth reserves the right to take legal action in the form of criminal as well as civil litigation.

§8 Rights of the Employee Council, data protection, ban on conduct- or performance-monitoring

(1) The Employee Council is authorized, with the approval of the University of Bayreuth's Data Protection Representative, to monitor whether the system administrators are adhering to data protection policy.

(2) Conduct- or performance-monitoring of employees shall not be carried out by the University of Bayreuth.

§9 Additional provisions

(1) Fees may be charged for using certain parts of the IT infrastructure.

(2) Additional user guidelines may be added for certain systems if needed.

§10 Legal validity

[1]These shall take effect on 1 December 2018. [2]These guidelines shall replace the Guidelines for the University of Bayreuth's IT Infrastructure dated 10 February 2005.

The University of Bayreuth is not liable for inaccuracies or mistakes in this English translation.
In case of doubt, the German originals are to be used in a court of law.