FH·W-S

University of Applied Sciences
Würzburg-Schweinfurt

University of Applied Sciences Würzburg-Schweinfurt

IT User Regulations

As of 14 March 2022

Contents

Preamble 3
Section 1 – Material scope 3
Section 2 – Personal scope and authorisation of use 4
Section 3 – User obligations 5
Section 4 – Tasks, rights and obligations of system operators 6
Section 5 – Exclusion and limitation of liability 8
Section 6 – Consequences of misuse or unlawful use 9
Section 7 – Additional regulations 9
Section 8 – Coming into effect 10

Preamble

The University of Applied Sciences Würzburg-Schweinfurt (FHWS) and its institutions (system operators) operate an information technology infrastructure (IT infrastructure) consisting of data processing systems (computers, servers), communication systems (networks) and other auxiliary information processing equipment. The IT infrastructure is connected to the X-WiN academic network and thus to the worldwide internet.

These IT User Regulations govern the conditions under which the IT infrastructure of the system operators and the associated range of services may be used.

The IT User Regulations

- are based on the legally defined tasks of the universities and on their mandate to safeguard the freedom of research and teaching,
- establishes basic rules for the proper operation of the IT infrastructure,
- point out the rights of third parties that must be protected (e.g. software licences, requirements of network operators, data protection and information security aspects) and
- obliges users to behave safely and correctly and to use the resources offered economically.

Sec. 1 – Material scope

(1) These User Regulations apply to the IT infrastructure provided by the system operators.

System operators are

a) the IT Service Centre (ITSC) of FHWS for central systems and services ,
b) the respective responsible organisational unit such as faculties, institutes, departments, Media Centre, Center Digital Education (ZDL), library or other organisational units of FHWS for decentralised systems.

(2) The User Regulations apply when internal services (e. g. internet, wireless LAN, the time recording system), FHWS systems, devices of FHWS or FHWS information are used. In addition, it applies to external services (e. g. the Virtuelle Hochschule Bayern vhb, supplier portals, Adobe) which are used in connection with the e-mail address of FHWS members, function e-mail addresses, or FHWS information. Separate terms of use apply to services such as BayernWLAN or eduroam that are not provided by the system operators.

(3) The IT infrastructure provided is available to users in accordance with Section 2(1) for the fulfilment of their tasks in teaching and research, education and further educa-

tion, university administration, central services, public relations and external presentation of the university and for other tasks described in Article 2 of the Bavarian Higher Education Act.

Sec. 2 – Personal scope and authorisation of use

(1) The User Regulations apply to all persons who use the IT infrastructure of FHWS (users). In particular, it applies to all organisational institutions (e.g. faculties, institutes, units, departments, central facilities) and all project organisations at all FHWS sites. Anyone wishing to use the IT infrastructure requires formal user authorisation from the responsible system operators. They may make the granting of the user authorisation dependent on proof of certain knowledge about the use of the IT infrastructure.

(2) Students and employees of FHWS automatically receive a role-specific user authorisation in the course of their enrolment or the establishment of their employment relationship. The user authorisation ends with the end of membership at FHWS (e.g. with de-registration or the end of the employment relationship).

(3) Other institutions and persons may be permitted to use the system by the system operators upon request, provided this does not restrict the use of the IT infrastructure by users pursuant to Para. 1, information security can be guaranteed and applicable laws are complied with. The university management shall commission the system operators to exercise this decision-making authority for their respective areas of responsibility. The authorisation to use the system shall end as soon as the reason for the authorisation to use the system has ceased to exist.

(4) The authorisation to use may be refused or restricted if

a) applicants do not fulfil their duties as users,
b) the capacity of the IT infrastructure, the use of which is requested, is not sufficient for the intended work due to an already existing workload,
c) the intended use is not compatible with the purposes pursuant to Section 1(3) and Section 3(1),
d) the IT infrastructure is obviously unsuitable for the intended use or is reserved for special purposes,
e) the IT infrastructure systems to be used are connected to a network which must meet special data protection requirements and no objective reason for this access request is apparent, or
f) it is not guaranteed that the requested use will not unreasonably interfere with other authorised uses.

(5) The user authorisation only entitles the user to work in connection with the requested use.

Sec. 3 – User obligations

(1) The IT resources referred to in Section 1(1) may only be used for the purposes specified in Section 1(3). Exceptions are as follows:

a) Minor use for private, but not commercial purposes is permitted after confirmation of this document and the regulations in the appendix to this document.
b) State support in the area of start-ups (e.g. EXIST funding) permits use in accordance with the statutes anchored therein and after confirmation of this document and the regulations in the appendix.
c) Use for other private commercial purposes may only be permitted upon written justified application and against payment; the university management shall decide on such an application.

Such use may not restrict the use of the IT resources for the purposes specified in Section 1(3).

(2) Users are obliged to ensure that they use the available resources (workstations, line capacities, hardware, software and consumables) responsibly and economically.

(3) Users are obliged to refrain from impairments of the operation, as far as they are foreseeable, and to avoid everything to the best of their knowledge that could cause damage to the IT infrastructure or to other users.

(4) Users are responsible for the access data they have been given. They are responsible for all actions that take place using their access data. This also applies if these actions are carried out by third parties, insofar as the users are responsible for this third-party use.

(5) Users are in particular obliged

a) to observe the information security guidelines provided by FHWS, in particular the guideline for information security and subordinate guidelines,
b) to inform themselves about the special terms of use of the respective software, documentation or data and to observe them as well as,
c) to comply with the relevant legal regulations (in particular copyright and data protection law) when using software (sources, objects), documentation and other data.

(6) Unless expressly permitted, software, documentation and data may neither be copied nor passed on nor used for purposes other than those permitted - in particular not for commercial purposes.

(7) Users shall refrain from any kind of misuse of the IT infrastructure. Misuse shall be deemed to have occurred in particular in the event of

a) violation of the reputation and the image of FHWS through detrimental dissemination of information and representations,
b) violations of information security and data protection regulations,

c) violation of copyrights or ancillary copyrights of third parties as well as other legal requirements,

d) disturbance or obstruction of other users or

e) use for commercial purposes, unless permitted.

(8) Users shall use the IT infrastructure in a legally correct manner. In particular, the following conduct is punishable:

a) spying on or intercepting data and corresponding preparatory acts (Section 202a-c StGB),

b) data alteration (Section 303a StGB),

c) computer sabotage (Section 303b StGB) and computer fraud (Section 263a StGB),

d) dissemination of propaganda material of unconstitutional organisations (Section 86 StGB) and incitement of the people (Section 130 StGB),

e) sexual offences under Sections 184 et seq. of the Criminal Code (in particular dissemination and possession and making available of pornographic writings and content),

f) insult or defamation (Sections 185 et seq. StGB),

g) copyright infringements, e.g. by unlawfully copying software or entering protected works and distributing them via the IT infrastructure (Sections 106 et seq. UrhG).

Even the attempt is punishable.

(9) Users are also prohibited from taking note of and/or using messages intended for other users without their consent.

(10) Users are obliged to coordinate a project for processing personal data with the system operators before it begins. The person responsible for data protection and information security for the respective faculty or central institution (“DISK”) as well as the Administrative Unit for Information Security and Data Protection shall be involved in this process. This does not affect the obligations arising from the provisions of data protection laws.

Sec. 4 – Tasks, rights, and obligations of system operators

(1) System operators shall keep documentation on the user authorisations granted.

(2) System operators shall make known the contact persons for the support of users.

(3) If necessary for troubleshooting, system administration and expansion or for reasons of system security and protection of user data, system operators may temporarily restrict the use of their IT systems or temporarily block individual users. If possible, affected users shall be informed of this in advance.

(4) System operators are entitled to check the security of the system/user passwords and the user end data by regular manual or automated measures and to initiate necessary protective measures, e.g. changes to easily guessed passwords, in order to protect the IT infrastructure and user end data from unauthorised access by third parties. Users must be informed immediately of any necessary changes to user passwords, access authorisations to user files and other protective measures relevant to use.

(5) In accordance with the following regulations, system operators are entitled to document and evaluate the use of the IT infrastructure by individual users, but only insofar as this is necessary

a) to ensure proper system operation,
b) for resource planning and system administration,
c) to protect the personal data of other users,
d) for accounting purposes,
e) for the detection and elimination of technical faults and errors, and
f) for the clarification and prevention of unlawful or improper use in the event of actual indications. These shall be documented in writing.

If stricter or additional requirements are to be complied with due to other regulations (e.g. IT works agreement), these shall apply with priority or as a supplement.

(6) System operators are also entitled to inspect the files of users in compliance with data secrecy, insofar as this is necessary to eliminate current malfunctions or to clarify and prevent illegal or abusive use, provided that there are actual indications of this.

However, inspection of the message and e-mail inboxes is only permissible insofar as this is indispensable to remedy current disturbances in the message service and can be justified under data protection law.

In any case, the inspection shall be documented and affected users shall be notified immediately as soon as this is possible without jeopardising the purpose of the measure.

(7) Under the conditions of Paragraph 5, connection and usage data in communication (especially e-mail usage) may also be documented. However, only the detailed circumstances of the telecommunication - but not the non-public communication contents - may be collected, processed and used.

The connection and usage data of online activities (in particular WWW usage) on the Internet and other teleservices which system operators make available for use or to which they provide access for use shall be deleted in accordance with the deletion periods provided for by law and within the framework of the principle of data economy.

(8) Insofar as there are factual indications that users violate these user regulations in a way that is

- criminally relevant

- unlawful or
- impairing the reputation or the image of FHWS

system operators may - within the limits of what is permissible under data protection law - order and implement provisional measures with regard to both the content and the user authorisation in order to prevent further illegal or abusive use until the legal situation has been sufficiently clarified. Those affected shall be informed of the measures immediately, as soon as this is possible without jeopardising the purpose of the measures. System operators shall inform the university management without delay of the existence of such indications and the ordering of provisional measures.

(9) In accordance with the legal provisions, the system operators staff shall be obliged to maintain telecommunications and data secrecy and shall be explicitly instructed on this by the system operator.

(10) To ensure proper operation, system operators may, in coordination with the IT Service Centre, make the use of special IT resources in the respective area of responsibility additionally dependent on specific pre-requisites.

(11) System operators are obliged to comply with the use and access guidelines of other operators when dealing with their IT resources.

(12) Within the scope of their processing activities, system operators shall ensure that the requirements of information security and data protection are complied with. In particular, any personal data collected during documentation and evaluation shall be deleted without delay as soon as the reason for collecting the data has ceased to exist.

Sec. 5 – Exclusion and limitation of liability

The system operators shall do everything in their power within the scope of the capacities available to them to ensure trouble-free operation with integrity. Liability in the following sense is excluded:

(1) The system operators and FHWS do not guarantee that the system functions meet the specific requirements of users and that the IT infrastructure is error-free and available at all times without interruption. The system operators cannot guarantee the integrity (in terms of destruction, manipulation) and confidentiality of the data stored with them.

(2) The system operators and FHWS do not assume any responsibility for the faultlessness of the systems provided. They are also not liable for the content, in particular for the correctness, completeness and topicality of the information to which they merely provide access for use.

(3) The system operators and FHWS are not liable for damages of any kind incurred by users from the use of the IT infrastructure. This does not apply in the event of injury to life, limb and health arising from the user relationship or due to the breach of essential obligations, i.e. obligations that make proper performance possible in the first place and on whose compliance the users may regularly rely from the user relationship. In the latter case, the claim shall be limited to the typical, foreseeable damage.

(4) Further claims shall remain unaffected by the above provisions.

Sec. 6 – Consequences of misuse or unlawful use

(1) The university management shall, after hearing the users concerned and after hearing the system operators, insofar as they have not already informed the university management of the factual indications and the ordered provisional measures in accordance with Section 4(8), take a final decision on the measures to be taken in order to remedy the abusive or unlawful use and to put a permanent end to it.

(2) In case of violations of legal regulations, of the provisions of these usage regulations, in particular of Section 3 (User obligations), or of other regulations of FHWS, the usage authorisation may be restricted or withdrawn for a limited period of time. It is irrelevant whether the violation resulted in material damage or not. In the case of serious or repeated violations, users may be permanently excluded from the use of all IT infrastructure.

(3) The aforementioned regulations shall not affect the university management's options to demand compensation from the users concerned for the damage caused by the misuse or illegal use and to counter this behaviour by means of disciplinary measures or to have it prosecuted by means of criminal charges. The other service and regulatory powers of the university management to which it is entitled against the members of FHWS also remain unaffected. If stricter or additional requirements are to be complied with due to other regulations (e.g. IT works agreement), these shall apply with priority or as a supplement.

(4) FHWS reserves the right to take legal action against users whose unlawful use of IT resources and user authorisation results in disadvantages for FHWS and its facilities, if users culpably fail to comply with their obligations under these user regulations.

(5) FHWS reserves the right to take legal action against users if third party use has caused disadvantages for FHWS and its facilities within the scope of the access and use options available to the users, if they are responsible for this third party use, in particular in the case of passing on their user ID to third parties.

(6) Users must compensate FHWS for any damages incurred.

Sec. 7 – Additional regulations

(1) The use of the IT infrastructure and services of the system operators is free of charge within the framework of these regulations, unless usage fees are to be charged according to special regulations which the system operators make in agreement with the university management.

(2) For certain systems, supplementary or deviating conditions of use may be laid down as required. Supplementary or deviating terms of use for staff members may also be contained in service agreements and/or service/employment/tariff regulations.

(3) Should parts of this user agreement be or become invalid, this shall not affect the validity of the remaining parts.

Sec. 8 – Coming into effect

The IT User Regulations come into force on the day of their announcement.

Würzburg, 14 March 2022

Prof. Dr. Robert Grebner
President

These regulations were set down on 14 March 2022 at the University of Applied Sciences Würzburg-Schweinfurt. This was communicated on 14 March 2022 by notice. The date of announcement is 14 March 2022.