General User Regulations (statutes) for the Communication and Data Processing Infrastructure of Europa-Universität Flensburg (IT User Regulations)

Dated June 12, 2018

Date of announcement in NBl. HS MBWK Schl.-H. 2018, page 42
Date of announcement on the EUF website: June 12, 2018

Pursuant to § 34.3 of the higher education act and law of the university hospital of Schleswig-Holstein (HSG), in the version published on February 5, 2016 (GVOBl. Schl.-H. p. 39), as last amended by the law of February 10, 2018 (GVOBl. Schl.-H. p. 68), the following statutes are enacted in accordance with the resolution adopted by the Presidium of Europa-Universität Flensburg on June 12, 2018:

Preamble

The purpose of these user regulations is to ensure that the communication and data processing infrastructure of Europa-Universität Flensburg (EUF) is as accessible, error- and interruption-free and secure as possible for those who use it. These regulations are based on the university's legally defined duties and responsibilities, and on its mandate to preserve academic freedom. They set basic rules for the proper use of the university's information processing infrastructure, and the user relationship between entitled persons (users) and Europa-Universität Flensburg.

§ 1 Sphere of validity

(1) These regulations govern the use of information processing infrastructure of Europa-Universität Flensburg, particularly the data processing equipment, communication systems, and other facilities for computer-aided information processing which the Center for Information and Media Technologies (ZIMT) runs and administers.
(2) The provisions of the Schleswig-Holstein Codetermination Act shall remain unaffected by these regulations.

§ 2 Legal status, organization and duties of ZIMT

(1) The legal status, organization, and duties of ZIMT are defined in its statutes.

(2) To ensure correct usage of the information and communication network and the data processing systems for which ZIMT is responsible, the head of ZIMT can, with assistance from the Staff Council (*Personalrat*), issue further technical and/or organizational regulations, such as those governing the use of the e-mail service, the ZIMT data network, or publications on ZIMT servers.

§ 3 Entitlement and permission to use

(1) EUF staff are entitled to use the IT services at EUF, for which they are granted permission upon their appointment or when they sign their employment contract. Permission can also be granted to:

1. Other members of the EUF community, as defined in § 13 HSG
2. Representatives of the university, for the purposes of executing official duties
3. Persons associated with facilities and institutions affiliated with EUF
4. Members of other universities, per special agreement
5. Other research and educational institutions and authorities associated with the German state of Schleswig-Holstein, per special agreement
6. The Schleswig-Holstein student union
7. Other legal or natural persons, per special agreement, provided that their usage is not detrimental to the interests of the group of persons listed in 1-6.

EUF reserves the right to restrict the group of persons entitled to use these services.

(2) Usage permission is granted solely for academic purposes with respect to research, teaching, studies, training, and for the execution of other EUF duties. Minor usage for other purposes is allowed if it does not go against the goals of ZIMT or the interests of the persons specified in paragraph 1.

(3) Permission to use the IT facilities and services of EUF is granted via a user permit. Students receive this permit when they enroll. In other cases, a permit can be obtained by application to the Presidium or a representative of the Presidium.

(4) Applications should be submitted via an application process specified by ZIMT.

(5) The user permit is valid only as long as the user's enrollment or employment at EUF, and/or only for the stated duration of the project for which the permit was request.

(6) To ensure that operation is correct and free of errors, user permits may be subject to a limitation of computing and online time, as well as other usage-related terms and conditions.

(7) ZIMT can also make the permission to use specific IT services conditional upon the user's possession of certain skills, competencies, or authorizations.

(8) If computing resources are insufficient to meet the needs of all authorized users, said resources may be allocated to individual authorized users in the order set out in § 1, since permission can only be granted within the boundaries imposed by the available resource capacities.

(9) The user permit can be denied, revoked or subsequently rescinded in whole or in part, in particular under the following conditions:

1. No formal application is submitted, or the information in the application is not or is no longer correct.
2. The conditions for proper use are not or are no longer present, especially due to technical defects in the data processing equipment.
3. The user is barred from using the facilities, in accordance with § 5.
4. The planned project is incompatible with the duties of ZIMT and with the purposes stated in paragraph 2.
5. The available data processing resources either do not suit the purpose for which they were requested, or are reserved for special purposes.
6. The requested resources are already in use and thus are insufficient to meet the needs of the planned project.

7. The data processing components to be used are connected to a network that must meet special data protection requirements, and there appears to be no objective reason for the planned project.
8. The requested use is likely to be unduly detrimental to other legitimate projects.

(10) The decision to take action on the basis of Paragraph 9 shall be made by the Presidium in consultation with the head of ZIMT, who shall act in an advisory capacity. The Presidium may delegate this task to an authorized person.

§ 4 User rights and obligations

(1) Entitled persons have the right to use the services and facilities, computer equipment, and information and communication systems of EUF under the terms of the user permit and in accordance with these regulations and those pursuant to § 2. Any use deviating from these conditions requires a separate permit.
(2) Users are required:

1. General
   a) To comply with the provisions of these regulations and observe the limitations of the user permit, in particular the purposes pursuant to § 3, paragraph 2
   b) To refrain from any activity that interferes with the proper operation of the IT equipment of EUF
   c) To handle all IT equipment, information and communication systems and other EUF facilities with care and consideration

2. User Identification
   a) To work solely with the user identification authorized to them under the terms of the permit
   (b) To ensure that no other person gains access to personal passwords, and to take measures to prevent unauthorized persons from accessing the computer resources of EUF. This includes protecting access to those resources by using a secret and appropriate (i.e., not easily guessed) password, which should be changed as regularly as possible
   c) Neither to divulge nor to use third-party user identifications and passwords
   d) Neither to gain unauthorized access to the information of third parties, nor to divulge, use, or change such information without permission

3. Software usage, Copyrights
   a) To use software, documentation and other data in accordance with legal requirements, in particular as regards copyright protection, and to observe the licensing conditions under which ZIMT provides software, documentation and data
   b) Neither to copy nor to divulge to third parties without permission the software, documentation and data provided by ZIMT, nor to use these for purposes other than those expressly permitted

4. Use of ZIMT facilities and computer labs
   a) To observe EUF house rules in ZIMT facilities, and to follow staff instructions if a rule is violated
   b) To show one's user permit upon request

(c) To report immediately to ZIMT all disruptions, damage or errors in IT equipment and data equipment belonging to ZIMT, without fixing these oneself
(d) Not to interfere with ZIMT-installed hardware, operating system configurations, system files, system-relevant files of authorized persons, or the network, except in agreement with ZIMT

5. Other
a) In justified individual cases, especially in the case of a justified suspicion of misuse or for troubleshooting purposes, to inform the head of ZIMT about the methods and programs used and give ZIMT access to said programs for control purposes
b) To avoid uncoordinated or unjustified excessive loading of the network to the detriment of third parties
c) To cooperate with the data protection officer (DPO) when handling personal data, and to take into consideration the data protection and data security precautions that she or he proposes, while upholding the obligations of users with respect to data protection.
(d) To comply with the data processing security guidelines of EUF

(3) The persons entitled to use the data pursuant to § 3 shall be specifically informed of the following criminal offences:
1. Data espionage (§ 202a StGB);
2. Data interception (§ 202b StGB);
3. Preparing to spy on or intercept data (§ 202c StGB);
4. Data modification (§ 303a StGB) and computer sabotage (§ 303b StGB);
5. Computer fraud (§ 263a StGB);
6. Dissemination of pornographic representations (§§ 184 ff. StGB), particularly the acquisition and possession of pedophilic depictions (§ 184b StGB) and dissemination of pornographic performances via radio or telemedia (§ 184d StGB);
7. Dissemination of propaganda materials of unconstitutional organizations (§ 86 StGB) and sedition (§ 130 StGB);
8. Personal offenses, such as insult or libel (§§ 185 ff. StGB);
9. Criminal copyright violations, e.g., copying software in violation of copyright (§§ 106 ff. UrhG).

§ 5 Exclusion from use
(1) Users may be temporarily or permanently restricted in their use of the data processing resources, or barred from using them, if they:
1. Culpably violate these user regulations, particularly the obligations listed in § 4 (abusive conduct) or
2. Misuse EUF data processing resources for the purpose of engaging in criminal offences
3. Cause disadvantages to EUF as a result of other kinds of illegal user activity or behavior (e.g. copyright or trademark infringements)
(2) Action pursuant to paragraph 1 shall only be taken after a prior unsuccessful warning. This shall not apply in the event of imminent danger, in which case the involved parties must be informed of said action without delay. The person or persons concerned shall be given the opportunity to respond.

(3) Temporary restrictions of use, which are decided on by the head of ZIMT, should be lifted as soon as proper use appears to have been restored.
(4) Permanent restriction of use or complete exclusion from further use will only be considered in the case of serious or repeated infringements within the meaning of paragraph 1, if future conduct is also unlikely to be proper. Decisions regarding permanent exclusion are made by the Presidium upon request from the head of ZIMT and after hearing from all involved parties. Possible claims of ZIMT arising from the usage relationship shall remain unaffected.

§ 6 Rights and obligations of ZIMT
(1) ZIMT administers all user permits granted, for which it maintains a central user file in which all necessary user data are collected and processed, for the purposes of ensuring proper data processing operations by ZIMT.
(2) Insofar as this is necessary for troubleshooting, system administration and expansion, or for reasons related to system security and the protection of user data, ZIMT may temporarily restrict the use of its resources or temporarily block user identifications. To the extent that this is possible, the persons concerned must be informed of this in advance.
(3) If there are sufficient grounds to believe that a user is holding illegal, ready-to-use content on EUF servers, the head of ZIMT can prevent further use of this content until the legal situation has been sufficiently clarified.
(4) To protect the IT resources and the user data from unauthorized access by third parties, ZIMT is entitled to check the security of the system/personal passwords and user data by means of regular manual or automated measures and to initiate necessary safeguards (for example, by changing easily guessed passwords). A change request can be directed to the authorized user. All parties concerned must be informed immediately of any necessary changes to personal passwords, access rights to user files, and other relevant safeguards taken by ZIMT.
(5) In accordance with the regulations listed below, the provisions of the (EU) Regulation 2016/679 (Basic Data Protection Regulation), the Schleswig-Holstein Data Protection Act, and other sector-specific data protection regulations, ZIMT shall be entitled to document the use of data processing systems by individual users and to process data, but only to the extent that this is necessary for

1. Ensuring proper system operation
2. Resource planning and system administration
3. Protecting the personal data of third parties
4. Accounting purposes
5. Detecting and eliminating errors
6. Investigating and preventing illegal or abusive usage

(6) Any data processing carried out in accordance with paragraph 5, for the purposes of inspecting or evaluating the data, can only take place with the involvement of the IT security officer(s) and data protection officer(s).
(7) Subject to the requirements of paragraphs 5 and 6, ZIMT is also entitled to inspect the files of specific users while respecting data secrecy, to the extent that this is necessary to eliminate current disturbances or to clarify and prevent abuses. However, this is only permissible if there are actual indications that such may be the case.
Message and e-mail inboxes can only be inspected if doing so is indispensable to solving current problems with the mail service.

In any case, the inspection must be documented and the user's immediate supervisor (head of department or service) must be immediately informed after the purpose of the inspection has been served. In the case of students, this function is performed by the EUF Vice-President for Studies and Teaching.
The department head informs the following parties of the inspection:

1. The person concerned
2. The members of the responsible staff council (*Personalrat*)
3. If necessary, the academic supervisor
4. If necessary, other persons, bodies, or committees

The head of department will then arrange for further action to be taken.
(8) Subject to the requirements of paragraphs 5 and 6, traffic and usage data with respect to communications (in particular email) can also be documented. However, only the more detailed circumstances of the telecommunications can be collected, processed and used not the non-public communication contents.
The traffic and usage data of the online activities on the Internet and other telemedia provided by ZIMT for use or to which ZIMT provides access for use, must be deleted as early as possible, unless it concerns accounting data.
(9) In accordance with legal provisions, ZIMT is obliged to maintain telecommunications and data secrecy.

§ 7 User liability

1. The user is liable for all disadvantages to EUF resulting from the improper or unlawful use of the university's data processing resources and user permit, or from the user's culpable failure to comply with her or his obligations, as set forth in these regulations.
(2) The user is also liable for damages caused by third party use in connection with the access and user privileges made available to her or him, if she or he is responsible for such third-party use, and particularly if said user has divulged her or his user ID or password to third parties.
(3) If, due to the user's abusive or unlawful conduct, third parties claim damages against EUF, seek cease-and-desist orders, or make any other claims, the user shall exonerate EUF from all such claims. EUF will notify the user of these proceedings, in the event that a third party takes legal action against it.

§ 8 Liability of the EUF

(1) EUF does not guarantee that the system will run problem-free and without interruption at all times. Possible data losses due to technical malfunctions as well as the illegal use of confidential data through unauthorized access by third parties cannot be excluded.
(2) EUF assumes no responsibility for the correctness of the programs it makes available. EUF is also not liable for the content, in particular for the correctness, completeness and topicality of the information to which it merely provides access for use.
(3) Furthermore, EUF shall only be liable in the event of intent and gross negligence on the part of its personnel, unless there has been a culpable breach of essential duties, the observance of which is of particular importance for achieving the purpose of the contract (cardinal duties). In this case, the liability of EUF is limited to typical damages foreseeable at the time when the usage relationship was established, unless intentional or grossly negligent action is involved.
(4) Possible official liability claims against EUF remain unaffected by the above provisions.

§ 9 Entry into force/expiry

(1) These statutes shall enter into force on the day following their publication.
(2) With the entry into force of these statutes, the previous user regulations of 29.10.1999 shall cease to apply.

Flensburg, 12. Juni 2018

Europa-Universität Flensburg
Prof. Dr. Werner Reinhart
President