

# **User Framework Regulation (Ordinance) for the Communication and Data Processing Infrastructure of Christian-Albrechts-Universität zu Kiel**

The following ordinance is enacted after the resolution passed on 11 November 2014 by the University Board of the Christian-Albrechts-Universität zu Kiel (hereafter referred to as "Kiel University") and after the resolution passed by on 17 December 2014 the Senate on the basis of Section 34 (3) of the law pertaining to higher education institutions and the University Medical Center Schleswig-Holstein (Higher Education Act (Hochschulgesetz – HSG)), which was promulgated on 28 February 2007 (Law and Official Gazette for the Land of Schleswig-Holstein (GVOBl. Schl.-H.), p. 184) and last amended by Article 1 of the Act from 4 February 2011 (GVOBl. Schl.-H, page 34, corrected GVOBl. Schl.-H. p. 67):

## **First Amendment from 18 December 2014 (Notices from the University Board, No. 94/2014)**

This version is an unofficial version for reading purposes only, in which the above mentioned amending ordinances have been incorporated. Only the text published in the Notices of the University Board continues to apply and be legally binding.

### **Preamble**

This User Regulation shall ensure insofar as possible the error-free, unimpeded and secure use of the communication and data processing infrastructure of Kiel University. This User Regulation is oriented toward the legal duties of the university, in particular its mandate to safeguard scientific freedom. It prescribes basic rules for the proper operation of the infrastructure for the processing of information and governs the user relationship between the individual users and the university.

### **Section 1 Scope of application**

This User Regulation applies to the use of both the central and decentralised communication and data processing infrastructure of Kiel University, consisting of data processing facilities, communication systems and other facilities for the computer-assisted processing of information.

Part 1: The central data processing infrastructure

### **Section 2 Legal status and internal organisation of the University Computing Centre**

(1) According to its constitutive ordinance, the University Computing Centre is a central institution of Kiel University.

### **Section 3 Duties of the University Computing Centre**

(1) The University Computing Centre must perform the duties pursuant to Section 1 (2) of its constitutive ordinance.

(2) The University Computing Centre is responsible for planning, installing and operating the computer-assisted information and communication systems. These include the required networks, central servers and data- and telecommunication systems. In this regard, the University Computing Centre has the following duties:

1. the provision and maintenance of the communication network operation without malfunction and where possible without interruption;
2. the coordination of the expansion and maintenance of the communication network;
3. the administration of address spaces and name spaces;
4. the provision of network services and central network servers; and
5. the support of users in the use of these services.

(3) The University Computing Centre is responsible for the procurement, management, documentation, maintenance and further development of standard and base software, in particular university and campus licenses.

(4) To ensure the proper functioning of the information and communication network and the data processing system allocated to the University Computing Centre, the management of the University Computing Centre may prescribe further technical/organisational rules governing the use of the data processing installations of the University Computing Centre, e.g. technical/organisational regulations pertaining to the operation of the data network and operational rules governing the use of the servers of the University Computing Centre.

(5) In the performance of its duties, the University Computing Centre is supervised by the University Board, advised by the advisory boards "Teaching, Services, Basic Services" ("Lehre, Services, Basisdienste") and "Scientific Computing, Digital Research Infrastructure" ("Wissenschaftliches Rechnen, digitale Forschungsinfrastruktur").

#### **Section 4**

##### **Right of use and authorisation of use**

(1) The following may be authorised to use the services of the University Computing Centre:

1. members of the university pursuant to Section 13 of the Higher Education Act;
2. persons employed by the university for the purpose of performing its duties;
3. members and associates of institutions affiliated with the university;
4. members and associates of other higher education institutions on the basis of special agreements;
5. other public research and educational institutions and authorities of the Land of Schleswig-Holstein or of the Federal Republic of Germany on the basis of special agreements;
6. the Studentenwerk (Student Union) of Schleswig-Holstein

(2) Authorisation will be exclusively granted for scientific purposes in the field of research, teaching and study, for the administration of the university, and for the purpose of training, further education and the fulfilment of any other legal obligations of Kiel University. Any other use (e.g. of a private, non-commercial nature) may be authorised provided that it is minimal and does not hinder the prescribed objectives of the University Computing Centre or inconvenience the other users.

(3) Authorisation to use the services and facilities of the University Computing Centre will be granted through the issue of a user license. This will be issued by the University Computing Centre in writing or electronically upon application by the user. A simplified procedure can apply for the use of special services.

(4) For applications under (3) Sentence 2, the University Computing Centre may request the following:

1. the name, address, student number and signature of the applicant;
2. a description of the purpose of use and/or proposed project;
3. an explanation of how the proposed project will be financed;
4. an explanation of how personal data will be processed;
5. an acknowledgement of this User Regulation and any payment rules;
6. a declaration of consent to the processing of the user's personal data;
7. a statement of the desired data processing resources.

(5) The user license is restricted to the project as stated in the application and may be limited in time.

(6) To ensure that the University Computing Centre can properly operate without malfunction, the user license may also be granted subject to restrictions upon the times when computers may be used and when users may go online, and subject to other terms and conditions of use.

(7) The University Computing Centre may authorise users subject to evidence of specific information pertaining to the use of the desired data processing systems and services.

(8) If the capacity of the resources is not adequate to satisfy the requirements of all authorised users, the resources available to individual users may be restricted through the implementation of a quota system.

(9) The user license may be wholly or partially refused or revoked, and may be subject to restriction after issue, particularly if

1. a correct application has not been made or the information provided in the application is no longer accurate;
2. the requirements for the proper use of the data processing facilities are not or no longer fulfilled;
3. the authorised user has been excluded from use under Section 6;
4. the project of the user is incompatible with the duties of the University Computing Centre and the purposes specified in Section 4 (2);
5. the existing data processing resources are not suited for the requested use or have been reserved for particular purposes;
6. the capacity of the resources, for the use of which the application is made, is not adequate for the planned use due to a pre-existing workload;
7. the data processing components that will be used are connected to a network that must comply with special data protection requirements and no objective reason for the planned use is apparent;
8. it is expected that the requested use will unreasonably prejudice the authorised use of other persons.

## **Section 5**

### **Rights and obligations of users**

(1) Users are entitled to use the University Computing Centre's facilities, its data processing facilities and information and communication systems within the framework of the user license and in accordance with the provisions of this User Regulation and any rules issued under Section 3 (4).

(2) Users are obligated to:

1. observe the provisions of this User Regulation and the restrictions imposed by the user license, in particular the purposes of use prescribed by Section 4;
2. refrain from any activity that may interrupt the proper operation of the University Computing Centre's data processing facilities;
3. treat in a careful and gentle manner all the University Computing Centre's data processing facilities, information and communication systems, and other facilities;
4. only work under the user ID that they have been authorised to use within the framework of the license;
5. ensure that the passwords allocated to user IDs are not disclosed to other persons;
6. neither ascertain nor use passwords pertaining to user IDs that were not allocated to them;
7. not access information belonging to other users without authorisation nor forward, use themselves or modify information acquired without permission;
8. observe legal provisions—in particular copyright laws—when using software, documentation and other data, and must observe the license conditions subject to which software, documentation and data is made available by the University Computing Centre;
9. refrain from copying or from forwarding to third parties, the software, documentation and data provided by the University Computing Centre unless expressly authorised to do so and must not use such materials for unauthorised purposes;
10. obey staff instructions when they are present on the premises of the University Computing Centre;
11. not remedy themselves any malfunctions, damage or faults sustained by the University Computing Centre's data processing facilities and data carriers but to promptly report such matters to the employees of the University Computing Centre;
12. not interfere with the University Computing Centre's hardware installations without the express consent of the University Computing Centre and not to modify the configuration of the operating systems, the system files, the users' system-relevant files or the network;
13. provide information relating to programmes and user methods on demand to the University Computing Centre's management for the purpose of supervision in individual cases—particularly where a well-founded suspicion of abuse exists or for the purpose of remedying malfunctions; and
14. agree to the processing of personal data with the University Computing Centre and—without prejudice to their own statutory duties to protect data—to observe the precautions regarding data protection and security that are proposed by the University Computing Centre.

(3) Particular reference is made to the following criminal offences:

1. data espionage, phishing and/or acts preparatory to data espionage and phishing (Sections 202 a, b and c of the German Criminal Code (Strafgesetzbuch – StGB));
2. data tampering (Section 303 a of the Criminal Code) and computer sabotage (Section 303 b of the Criminal Code);
3. computer fraud (Section 263 a of the Criminal Code);
4. acquisition, possession and distribution of pornographic images (Section 184 and Sections 184 a–d of the Criminal Code);
5. dissemination of propaganda material of unconstitutional organisations (Section 86 of the Criminal Code) or incitement to hatred (Section 130 of the Criminal Code);

6. offences that damage reputation, such as insult or intentional defamation (Section 185 et seqq. of the Criminal Code);
7. criminal violations of copyright law, e.g. the duplication of software in breach of copyright (Section 106 et seqq. of the German Copyright Act (Urhebergesetz – UrhG)).

(4) Reference is made to the German Information and Communication Services Act (Informations- und Kommunikationsdienstegesetz) und the Interstate Treaty on Media Services (Mediendienste-Staatsvertrag).

## **Section 6**

### **Exclusion from use**

(1) Users may be temporarily or permanently restricted in their use of data processing resources or may be excluded from such use if they culpably infringe the provisions of this User Regulation, in particular by breaching the obligations prescribed by Section 5 (abusive conduct).

(2) The measures stipulated under (1) will only be taken with the consent of the Dean of the relevant faculty after a prior unheeded warning has been issued. The affected party is to be granted an opportunity to state his/her case. He/she may request the mediation of the Chairperson of the advisory boards "Teaching, Services, Basic Services" and "Scientific Computing, Digital Research Infrastructure". In any case, the data belonging to the affected party will be saved.

(3) Any temporary restriction of use, on which the management of the University Computing Centre is to decide, is to be lifted as soon as it appears that proper use is again assured.

(4) Users may only be permanently restricted or completely excluded from further use in the case of serious or repetitive breaches within the meaning of (1) even where proper future use is not anticipated. The decision to permanently exclude will be made by order of the University Board upon the application of the management of the University Computing Centre after the advisory board "Teaching, Services, Basic Services" and/or "Scientific Computing, Digital Research Infrastructure" has been heard.

## **Section 7**

### **Rights and obligations of the University Computing Centre**

(1) To ensure proper administration, the University Computing Centre will keep information in its systems regarding the user authorisations that it has issued.

(2) The University Computing Centre may temporarily restrict the use of its resources or temporarily block the user IDs of individual users if such action is necessary for reasons of system security or for the purpose of remedying malfunctions or in order to administer or extend the system or protect user data. Users affected by such restrictions should—if possible—receive advance notification.

(3) If there are factual indications that a user may be storing unlawful content on the University Computing Centre's servers for the purpose of its use, the University Computing Centre may prevent further use until the legal position has been adequately clarified.

(4) The University Computing Centre may examine the security of the user's systems, data and passwords through regular manual or automated measures and may implement necessary protective measures—e.g. the modification of easily guessed passwords—in order to protect data processing resources and users' data from unauthorised third party access. Users must be promptly notified of any necessary modification to their passwords, access authorisations to their files and of any other user-relevant protective measures.

(5) The University Computing Centre may document and evaluate the utilisation of the data processing systems by individual users in accordance with the following rules if this is necessary in order

1. to ensure that the system functions properly;
2. to plan resources and administrate the system;
3. to protect the personal data of other users;
4. for billing purposes;
5. to identify and remedy malfunctions; and
6. to clarify and prevent unlawful use or abuse.

(6) In accordance with the criteria prescribed by (5) — and subject to the observance of data confidentiality—the University Computing Centre may also inspect the users' programmes and files, insofar as this may be necessary in order to remedy existing malfunctions or to clarify and prevent abuse where there are factual indications for such an abuse. The inspection is always to be documented and the relevant user is to be promptly informed once its objectives have been attained.

(7) Subject to the criteria prescribed by (5), the connection and user data pertaining to the exchange of messages—particularly with regard to e-mail use—may also be documented. However, only the details concerning the circumstances of the telecommunication—and not the private contents of communications—may be compiled, processed and used. The connection and user data pertaining to online activities over the Internet or through other teleservices whose use is provided—or rendered accessible—by the University Computing Centre are always to be deleted as quickly as possible and in any event by no later than directly after the termination of the relevant use unless required for billing purposes.

(8) The University Computing Centre is obligated to keep data and telecommunications confidential pursuant to the statutory provisions.

## Part 2: Decentralised data processing infrastructure

### **Section 8**

#### **Terms and conditions of use**

(1) The use of the decentralised communication and data processing infrastructure provided and operated may be regulated by the relevant responsible institutions who may determine user authorisations and the manner and duration of use. To ensure that facilities and equipment operate without malfunction, the operator may restrict use to the extent required for this purpose.

(2) In exceptional cases, special user rules applicable to the decentralised communication and data processing infrastructure can be authorised by the University Board.

## Part 3: General provisions

### **Section 9**

#### **Liability of the user**

(1) The user (Section 4 (1)) is liable under general provisions of German civil and employment law.

(2) The user is liable for loss and damage arising from third party use that occurs within the framework of possibilities of access and use provided to him/her in circumstances where he/she is responsible for the said third party use, particularly where his/her user ID has been disclosed to the relevant third party.

## **Section 10**

### **Warranty and liability of the university**

(1) The university does not warrant that the system will be free of faults and will operate without interruption at all times. It cannot be excluded that data might be lost due to technical malfunction or that confidential data might be disclosed through the unauthorised access by third parties.

(2) The university does not assume any liability that the programmes it provides will be free of faults.

(3) The university is only liable for loss and damage which has been caused by itself or its vicarious agents by intent or gross negligence. Personal injury is subject to statutory provisions.

Kiel, 18 December 2014

Signed  
Prof. Dr Lutz Kipp  
President