Regional Computing Center Regulations for Use

Universität Hamburg Administrative Directive dated June 2005

As Director of the Regional Computer Center, I hereby issue the following Regulations for Use as an administrative directive for the Regional Computer Center at Universität Hamburg Prof. Dr.-Ing. Karl Kaiser

Preamble

These Regulations for Use are intended to ensure the most uninterrupted, unhindered, and secure use possible for RRZ communications and IT infrastructure. The Regulations for Use are based on the statutorily defined tasks of Universität Hamburg as well as on its mandate to preserve academic freedom. They establish basic rules for proper operation of the IT infrastructure and thus govern the usage relationship between individual users and RRZ.

Section 1 Scope

These Regulations apply to the use of RRZ's information processing infrastructure, consisting of the data processing equipment, communications systems, and other computer-based information processing equipment under RRZ's control. With respect to employees at Universität Hamburg, employment and civil service provisions take precedence over these Regulations for Use in cases of any conflict.

Section 2 Authorization and access for use

1. The following may utilize RRZ services:

    a. members, affiliates, and institutions including the central administration at Universität Hamburg;

    b. representatives from Universität Hamburg so they may perform their commissioned duties;

    c. members of other universities of the Free and Hanseatic City of Hamburg (FHH) or state universities outside the FHH on the basis of special agreements;

    d. other state research and educational institutions and FHH authorities on the basis of special agreements;

    e. student services in FHH;

    f. other legal entities or natural persons, provided that the interests of the users named under a. to e. are not affected.

2. Access shall be granted exclusively for academic purposes in research, teaching and study, for purposes of the library and university administration, education and training, and for the

performance of other tasks of Universität Hamburg. Additional uses may be only permitted where the use is minor and will not impair the purpose of RRZ or the interests of other users. Commercial application and use is not permitted.

3. Access to use the facilities and services of RRZ is granted through user authorization. This is issued by RRZ in writing upon the request of the person desiring access for use.

4. The application should contain the following information on a form provided by the Regional Computing Center:

a. name, address and signature of the applicant as well as the applicant's status as either a student, employee, institution, or other user as defined in no. 1 of these Regulations;

b. description of the intended use or proposed project;

c. desired DP resources;

d. a declaration of consent corresponding to the extent personal data will be processed;

e. acceptance of these Regulations for Use and the Rules of Operation issued by RRZ as the basis of the agreement of use;

f. acknowledgment of the cost and fee schedule as amended.

Additional information may only be collected to the extent necessary to make a decision on the application for the grant of access.

5. Use authorization is limited to the project specified in the application or by semester in the case of personal student identifiers; and may otherwise be limited in duration.

6. In order to ensure proper and uninterrupted operation, authorization for use may also be combined with a limitation of the computing and online time as well as other use-related conditions and requirements.

7. Furthermore, RRZ may make access conditional on the provision of proof of certain knowledge by the user on how to use the desired data processing systems and data processing services.

8. If DP resource capacity is not sufficient to meet the needs of all authorized users, operating resources may be allocated to individual users in the order of priority established in no. 1 of these Regulations.

9. Authorization for use may be denied, revoked, or subsequently restricted, in whole or in part, in particular if

a. a proper application has not been submitted or the information in the application is not or is no longer accurate;

b. the requirements for proper use of the data processing facilities are not or are no longer met;

c. the person authorized to use the facilities has been excluded from use in accordance with Section 4;

d. the planned project of the person using the facilities is not compatible with the tasks assigned to RRZ and the purposes stated in no. 2;

e. the existing data processing resources are unsuitable for the requested use or are reserved for special purposes;

f. the capacity of the resources sought to be used is insufficient for the planned use because of an existing workload;

g. the data processing components to be used are connected to a network that must meet special data protection requirements and no objective reason for the planned use is apparent;

h. the requested use is expected to unreasonably interfere with other legitimate projects.

Section 3 User rights and obligations

1. Authorized users have the right to use the facilities, data processing systems, and information and communication systems of RRZ within the scope of their respective authorization for use and in accordance with these Regulations for Use.

Any other use requires separate approval.

2. Users must

a. comply with the provisions of the Regulations for Use and observe the limits of the authorization of use, in particular observe the purposes of use according to Section 2 no. 2;

b. refrain from anything that interferes with the proper operation of the data processing facilities of RRZ or third parties;

c. treat all data processing equipment, information and communication systems, and other facilities of RRZ with care and consideration;

d. exercise special care when using private systems and operating them on the communications network of Universität Hamburg;

e. work exclusively with the usernames issued for access;

f. ensure that no other persons gain knowledge of user passwords, and take precautions to prevent unauthorized persons from accessing RRZ's data processing resources; this includes protecting access by means of a password that is to be kept secret and that is suitable, i.e. not easy to guess, and which should be changed as regularly as possible;

g. not attempt to discover or employ the usernames or passwords of others;

h. not attempt to gain unauthorized access to the information of other users and not pass on, use, or change the information of other users without permission;

i. comply with legal requirements when using software, documentation and other data, in particular requirements regarding copyright law, and observe the licensing conditions under which such software, documentation and data are made available by RRZ;

j. not copy or pass on software, documentation and data provided by RRZ to third parties, unless expressly permitted, nor use them for purposes other than those permitted;

k. follow the instructions of the staff while on the premises of RRZ and observe RRZ house rules;

l. provide proof of authorization for use upon request;

m. not attempt to fix malfunctions, damage, and errors on data processing equipment and data storage devices of RRZ, but rather report such immediately to RRZ staff;

n. not tamper with RRZ's hardware installations and not modify the configuration of the operating systems, system files, system-relevant user files, and the network without RRZ's express consent;

o. on justified request, for purposes of control, provide RRZ's management with information on programs and methods that have been used, and permit inspection of the programs—especially in the event of the justified suspicion of improper use as well as for troubleshooting purposes;

p. coordinate any processing of personal data with RRZ and take into account the data protection and data security precautions proposed by RRZ, without prejudice to the user's own obligations under data protection law;

3. Attention is directed specifically to the following crimes:

a. data espionage (Section 202a of the German Criminal Code (Strafgesetzbuch, StGB));

b. data manipulation (Section 303a StGB) and computer sabotage (Section 303b StGB);

c. computer fraud (Section 263a StGB);

d. dissemination of pornography (Section 184 StGB), in particular retrieval or possession of child pornographic images (Section 184 (5) StGB);

e. dissemination of propaganda material of unconstitutional organizations (Section 86 StGB) and incitement of the masses (Section 130 StGB);

f. honor offenses such as verbal assault or defamation (Sections 185 et seq. StGB);

g. criminal copyright infringements, e.g. by copying software in violation of copyright law (Sections 106 et seq. German Act on Copyright and Related Rights (Gesetz über Urheberrecht und verwandte Schutzrechte, UrhG)).

Section 4 Exclusion from use

1. Users may be temporarily or permanently restricted in their use of data processing resources or excluded from such use if:

a. they culpably violate these Regulations for Use, in particular the obligations listed in Section 3 (conduct in violation) above, or

b. there is strong probable cause to believe that users are improperly using computer center resources for criminal acts, or

c. the higher education institution is adversely affected by virtue of other illicit user behavior,

d. the user is uncooperative when malfunctions are being rectified (for example, by disregarding or failing to promptly undertake instructions provided by RRZ staff to eliminate malfunctions).

2. Users must be given a warning prior to measures pursuant to no 1 being taken, unless for conduct pursuant to Section 3 no. 3, or where appears necessary to maintain trouble-free operation. The user must be afforded the opportunity to be heard on the matter. He/she may ask the mediator of the Senate Committee on Data Processing to mediate. In any case, the user must be given the opportunity to secure their data.

3. A decision regarding the temporary restriction of use by the RRZ Director or an authorized RRZ staff member shall be rescinded once proper use again appears to be guaranteed.

4. A permanent ban on use or the complete exclusion of a user from further use is only possible in the case of serious or repeated violations as defined in no. 1, when proper conduct can no longer be expected in the future. A formal administrative decision on a permanent ban shall be decided by the head of administration upon an application submitted by the RRZ Director and subsequent to a hearing before the senate committee for data processing (Senatsausschuss Datenverarbeitung, SenA-DV). This shall not affect any other RRZ claims arising from or in connection with the user relationship.

Section 5 RRZ rights and obligations

RRZ maintains user files containing allocated user authorizations, which include usernames and email identifiers, resources authorized for use, and the names and addresses of authorized users.

1. To the extent necessary for troubleshooting, system administration and expansion, or for reasons of system security and protection of user data, RRZ may temporarily restrict the use of resources or temporarily block individual usernames. If possible, affected users will be informed prior to any action taken.

2. If there are actual indications that a user is providing illegal content for use on RRZ systems, RRZ may prevent further use until the legal situation has been sufficiently clarified.

3. RRZ is entitled to check the security of system/user passwords and user data as well as the security of systems connected to the Universität Hamburg network by means of regular manual or automated measures and to implement necessary protective measures, e.g. changes to easily guessed passwords, in order to protect DP resources and user data from unauthorized access by third parties. Users or third parties responsible for an area that has been affected must be promptly informed if it is necessary to change user passwords or access authorizations to user files or otherwise undertake other protective measures relevant to use.

4. In accordance with the following provisions, RRZ is entitled to document and evaluate the use of the data processing systems by the individual persons using them, but only to the extent that this is necessary

a. to ensure proper system operation;

b. to protect the personal data of other users;

c. for accounting purposes;

d. for the detection and elimination of malfunctions or

e. to clarify and prevent illegal or improper use.

5. RRZ is also entitled, under the conditions of no. 4 above, to inspect the user files in compliance with data secrecy, insofar as this is necessary to eliminate current malfunctions or to clarify and prevent improper use, provided that there are actual indications to reasonably believe this is necessary.

However accessing messaging and email mailboxes is only permissible if this is indispensable to rectify current faults in the messaging service.

Any and all access must be documented and the user affected must be promptly notified once the purpose of the access has been completed.

6. Under the conditions of no. 4 above, the connection and usage data in communications (especially email usage) may also be documented. However, only the specific instances of telecommunication and not the non-public communication contents may be collected, processed, and used. To prevent viruses and spam attacks, RRZ is entitled to use appropriate technical measures (e.g. virus scanners and spam filters).

The connection and usage data of online activities on the internet and other telecommunication services that the computing center provides for use or to which the computing center provides access for use will be deleted as soon as possible, unless this concerns billing data.

7. In accordance with statutory provisions, RRZ must maintain telecommunications and data secrecy.

Section 6 User liability

1. Users shall be held liable for all adverse effects suffered by Universität Hamburg as a result of or arising from improper or illegal use of data processing resources and user

authorization attributable to users negligently failing to comply with their obligations arising from these Regulations for Use.

2. Users shall also be held liable for any and all damage or loss caused by a third party's use of the data processing system, provided that such third party access and use is attributable to the conduct of the user; especially in cases where usernames have been passed on to third parties. In such a case, Universität Hamburg may charge the user a fee for third-party use in accordance with fee regulations.

3. Users shall indemnify and hold Universität Hamburg harmless against any and all claims if third parties assert claims for damages, injunctive relief, or otherwise against Universität Hamburg on account of improper or unlawful conduct on the part of users. To the extent any third party has taken legal action against RRZ, Universität Hamburg will add that user to the claim.

Section 7 Universität Hamburg liability

1. Universität Hamburg does not warrant that systems will run error-free and without interruption at all times. Possible data loss as a result of technical malfunctions as well as the discovery of confidential data through unauthorized access by third parties cannot be entirely excluded.

2. Universität Hamburg assumes no responsibility for the accuracy of the programs that are supplied. Universität Hamburg shall also not be held liable for content, in particular for the accuracy, completeness, and actuality of information to which it merely provides access for use.

3. Universität Hamburg assumes no liability for damage or loss to private systems that use Universität Hamburg's communications network.

4. This notwithstanding, Universität Hamburg shall only be held liable for cases of intentional misfeasance and/or gross negligence on the part of its employees and a negligent breach of material cardinal obligations. In such cases, Universität Hamburg's liability shall be limited to typical damage or loss foreseeable at the time of the establishment of the user relationship, insofar as such is not attributable to intentional or grossly negligent conduct.

5. This shall not affect any right to assert claims for liability against Universität Hamburg.