Guidelines for use of information-processing systems belonging to the University of Erlangen-Nuremberg

1. Sphere of validity of the guidelines for use

These guidelines for use are valid for computers, communication networks and other aids to information processing, which, within the framework of the tasks assigned by law to colleges and universities (cf. Article 2 of the Bavarian Colleges and Universities Law [BayHSchG]) are made available at the Regional Computing Centre in Erlangen [RRZE] and the University of Erlangen-Nuremberg for the purposes of information processing. These guidelines regulate the use and uses of these computer systems, in particular the rights and duties of the user and the roles of the system operator.

2. Authorised Colleges and Universities

- With regard to the facilities offered by the Regional Computing Centre Erlangen [RRZE], the universities of Erlangen-Nuremberg, Bamberg and Bayreuth, and the colleges of Nuremberg and Coburg are the authorised users.
- With regard to other facilities the University of Erlangen-Nuremberg is the authorised user.

3. Authorised individuals

1. All members of the authorised colleges and universities are entitled to use the facilities referred to in Section 1, above. It is possible for other individuals to be permitted to use the facilities referred to.
2. Members of the University of Erlangen-Nuremberg should approach the Regional Computing Centre Erlangen [RRZE], or the organisational unit responsible for them.

4. Formal authorisation of use

1. Anyone wishing to use the facilities referred to in section 1 requires formal authorisation from the system operator responsible. Anonymous services are excepted.
2. The system operators are
   1. the Regional Computing Centre Erlangen [RRZE] which is responsible for centralised systems,
   2. the individual organisational units such as faculties, institutes, operating units, professorial chairs and other sub units of the University of Erlangen-Nuremberg. These are responsible for decentralised systems.
3. The request for a formal authorisation must contain the following information:
   1. Operator/Institute or organisational unit
   2. System
   3. Name and address of user
   4. Brief description of purpose of proposed use, e.g., undergraduate essays/ graduate thesis / research / teaching / training
   5. A declaration of user's acceptance of guidelines for use
   6. Entries for the university's information service

The system operator may ask for further details only when such details have a direct and urgent bearing on the decision whether to authorise use.

4. Decisions regarding formal authorisation of use lie with the system operator responsible. The system operator can make the authorisation of use dependent on proof of a certain level of competence in using the computer or system in question.
5. Authorisation may be refused only
    1. when it seems unlikely that the prospective user will fulfil the required duties of a user;
    2. or when the capacity of the computer for which an application for use is being made will not, because of current levels of use, be sufficient to enable the intended work to be conducted;
    3. or when the intended use conflicts with the purposes expressed in section 5 paragraph i.
6. The authorisation of use authorises only such work as is relevant to the purpose for which the request for use was made.

5. The user’s general duties

1. The facilities referred to in Section 1 may be used only for the purposes defined by law. Use for any other purpose, in particular for private or commercial purposes, must be specially authorised and must be paid for.
2. The duties of the user are as follows:
    1. To ensure that the operating facilities (work space, computer capacity, hard-disk memory, line capacity) are used responsibly since they are in short supply.
    2. To work only under her / his own user-identity.
    3. To protect access to the facilities through the use of a confidential password or similar tools or procedures.
    4. To take steps to ensure that unauthorised third-parties cannot gain access to the facilities. Such steps would include the avoidance of over-simple or easily guessable passwords, the regular alteration of passwords, and taking care not to forget to log out.
    5. To adhere closely to the user and access guidelines of other operators in the course of interaction with them.

The user is solely and fully responsible for all actions taken under her / his user- identity.

6. Further user duties

1. Further user duties are
    1. to refrain from using any software whatsoever other than that provided by the operator or developed by the user her/himself,
    2. to adhere strictly to the conditions for the use of software acquired and made available by the operator, software which may be under licence,
    3. to refrain from copying or passing on software or using it for purposes other than those permitted, particularly for private or commercial purposes, unless such software is clearly marked as freeware.
2. Without the express agreement of the operator responsible the user is forbidden
    1. to install software other than that made available by the operator,
    2. to make alterations to the hardware installation,
    3. to make alterations to the configuration of the operating system or the network.
3. The user is obliged to discuss and agree upon any processing of personal data with the operator before commencing with such work. Such discussions and agreements do not release users from the obligations arising from the data protection laws.
4. The user is obliged to adhere to the relevant guidelines for use, such as the guidelines for using networks or guidelines on ethical and legal use of software.
5. Each user is responsible for the effects of the programmes which she/he runs. The operator has a duty to inform her/himself sufficiently, and in advance, of the possible effects of the programme.

7. Operator liability/Exemption from liability

1. The system operator does not guarantee that the functions of the system will meet the special needs of the user, nor that the system will operate without errors or without interruptions.

2. The system operator is not liable for damage of any kind arising from the use by the user of the facilities referred to in Section 1. The exception is wilful behaviour on the part of the operator or those persons whom the system operator uses as agents in the fulfilment of the operator’s tasks.

8. The consequences of improper or of illegal use

1. The system operator can limit use or withdraw authorisation completely when there has been illegal use of the system or a breach of these guidelines, and if it seems that the user is unlikely to adhere to the guidelines, in particular in the following ways:
    1. if there has been improper use of the facilities referred to in Section 1 for purposes other than those permitted,
    2. if there has been an attempt to discover other people’s passwords,
    3. if there has been an attempt to hack into other systems, data bases or computer networks, or
    4. there has been a violation of copyrights.

With regard to this it is immaterial whether or not the violation of the law or the non-adherence to guidelines has caused substantive damage.

2. Where there are serious or repeated violations, the user in question can be banned permanently from use of all the facilities referred to in Section 1 if her or his behaviour indicates that adherence to the guidelines cannot be expected. The Regional Computing Centre Erlangen [RRZE] will be responsible for taking such decisions within the complete sphere of validity of the guidelines.
3. Irrespective of the decisions made in accordance with paragraphs 1 and 2, the case for criminal and civil proceedings is always to be examined. The system operators are obliged to pass on to the legal department of the university’s central administration department [ZUV] any important information relevant to criminal or civil proceedings. The central administration department [ZUV] will then consider if and how to proceed further.

9. The role of the system operator

1. Each system operator will keep a documentary record of the user authorisations issued and of the assignment of operating equipment and facilities (privileges, resources). This documentation on user authorisation must be kept for a period of at least two years after the expiry of that authorisation. The operator is obliged to maintain confidentiality.
2. Before agreeing to the use of software suggested by the user, the operator must check that the use of such software with the computers in question is safe and whether, in terms of patent rights, the user is entitled to use the software.
3. The system operator is entitled
    1. to document the activities of the user in so far as this seems necessary to discover and identify cases of incorrect or improper use,
    2. to examine a user’s data if there are concrete grounds for suspicion that there has been improper use of facilities.
4. The system operator is, furthermore, entitled to make random tests to ensure that the facilities are not being used improperly. The system operator will identify to the user the contact person who will assist and support the user. The operator will, when required, also publish further and complementary guidelines for use.

Please note: Although this is a careful translation from the German, it is the German text alone which is legally binding.

Stand: 2. Juni 1995
Universität Erlangen-Nürnberg, Kommission für Rechenanlagen (KoRa)