Usage Regulations
for the Information Processing Systems of the
Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities

The Bavarian Academy of Sciences and Humanities hereby issues the following Usage Regulations. They describe the conditions under which the products and services of the Leibniz Supercomputing Centre may be used.

Preamble

The Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities (LRZ; LRZ is the German abbreviation for Leibniz-Rechenzentrum) operates an information processing infrastructure (IT infrastructure) consisting of data processing systems (computers and storage), communication systems (networks), other auxiliary information processing systems and the services based on them. The IT infrastructure is integrated in the German National Research and Education Network (DFN WiN) and is thereby integrated in the worldwide Internet.

The Usage Regulations are intended
  - to establish basic guidelines for the proper operation of the IT infrastructure
  - to ensure that the rights of third parties are protected (e.g. software licenses, network operator requirements and aspects of data protection and security)
  - to oblige users to use the supplied resources responsibly and economically
  - to inform the users about the measures that may be taken in the event of violations of the Usage Regulations.

§ 1 Area of validity

These Usage Regulations are valid for the IT infrastructure provided by LRZ.

§ 2 Individuals and institutions with right of use

  (1) The right of use is applicable to the following:

  a) with reference to the **_national supercomputer_** procured for scientific institutions, research groups and national Grid infrastructures: the members and associates of all German public institutions of higher education and scientific institutions in Germany which are predominantly state-funded,

b) with reference to the ***high-performance systems procured for all Bavarian institutions of higher education***: all associates and members of the Bavarian institutions of higher education,

c) with reference to the ***LRZ's other IT resources***: the Technische Universität München and the Ludwig-Maximilians-Universität München.

d) Scientists of other European scientific institutions may also be granted access to the LRZ's IT infrastructure in the course of European projects – taking into consideration the needs of the users with priority referring to the articles of incorporation. Insofar as products and/or services of the Computer Centre are used of without reimbursement of expenses, appropriate counter-performance or another form of compensation shall generally be provided for.

(2) The LRZ's IT infrastructure is available to the members of the institutions of higher education holding rights of use to carry out their work in the areas of research, teaching, education and training, public relations work and promotional activities of the institutions of higher education and other work described in Art. 2 of the Bavarian Higher Education Act (Bayerisches Hochschulgesetz). If necessary, the resources are also available to the administrations of the institutions of higher education holding rights of use insofar as they have no other way to carry out these tasks.

(3) Other individuals and institutions closely associated with science may receive permission to use this infrastructure on the basis of a service catalogue, insofar as such use does not interfere with the use of the priority users mentioned in § 2 (1).

§ 3 Formal user authorisation

(1) Anyone wishing to use the LRZ's IT infrastructure must obtain a formal user authorisation from the LRZ. The following are excepted:

- Authorisations for basic services (such as access to the Munich Scientific Network, email, file services), the issue of which has been delegated to individual institutions with which the data relating to the user account and personal data are checked and compared automatically;
- Authorisations for which anonymous access has been set up (e.g. information services, library services, short-term user accounts for guests at conferences);
- Authorisations for special computers as part of Grid services (such as in projects D-Grid, DEISA), the issue to participating institutions of which has been delegated and the users of which explicitly declare their willingness to adhere to the corresponding *Acceptable Use Policies* (such as in projects EGEE or DEISA).

(2) A so-called "LRZ Project", which the head of the respective institute can apply for, is required for use of the LRZ services as a formal framework, aside from the exceptions referred to in § 3 (1). When submitting an application, one or more individuals who are in charge of the project (so-called "Master Users") must be designated as contacts for the LRZ.

(3) Each institute, which grants authorisations without a single-case decision by the LRZ (e.g. when a new employee is hired or when students register, by Master Users or designated individuals for data processing), must make sure that the users engage to adhere to these Usage Regulations.

(4) The application for a user authorisation must contain all of the data requested on the corresponding form.

(5) The LRZ shall decide on the application. It can make the user authorisation contingent upon proof of specific know-how relating to the use of the system.

(6) The user authorisation may be refused if

a) the applicant's compliance with its duties as a user (§ 4) does not appear to be ensured;
b) the capacity of the resources which use is being applied for is not sufficient, because they are already being used to full capacity for the intended work;

c) the project is not compatible with the purposes pursuant to § 2 (2) and (3) and § 4 (1);
d) the resource is obviously not suited for the intended use or is reserved for special purposes;
e) the resource to be used is connected to a network for which special data protection requirements must be met, and there is no objective reason for this request of access;
f) it appears that other uses will be disturbed unreasonably as a result of the use being applied for.

(7) The user authorisation can be withdrawn or restricted temporarily or permanently if

a) one of the reasons for rejection pursuant to § 3 (6) occurs or is discovered subsequently;
b) the user uses LRZ's IT infrastructure for criminal offences or causes harm to the institution of higher education/institute due to another illegal act;
c) the restriction of use is absolutely necessary in order to resolve reasonable suspicion of serious misconduct;
d) the user/the institution defaults in payment for the use for a period of more than two months and does not pay on time despite a reminder and a deadline for payment.

The steps according to this provision shall not be taken until after a prior warning was ignored. The affected party has the right to reply to the accusations. The party shall be permitted an opportunity to save its data. Temporary restrictions of use will be removed if proper use appears to be guaranteed.

(8) The user authorisation only authorises the holder to do work that is related to the use applied for.

§ 4 The user's obligations

(1) The LRZ's IT infrastructure may only be used for the purposes mentioned in § 2 (2) and (3). The user must refrain from any form of abusive use of the IT infrastructure.

(2) The user is obligated to make sure that he or she uses the existing equipment (workstations, CPU capacity, disk space, line capacity, peripheral devices and consumables) responsibly and economically. Users are obligated to avoid any foreseeable operational disturbances, and, to the best of their knowledge, refrain from any activities which might cause damage to the IT infrastructure or other users.

(3) The Computer Centre can issue policies for specific user groups, as well as requirements and instructions in an individual case. In particular, the user is obligated to

a) exclusively work with the user accounts, the use of which has been permitted to him or her. Passing on of user accounts and passwords is generally not permitted;
b) protect the access to LRZ's IT infrastructure by a password which must be kept secret or by an equivalent procedure;
c) Take precautions so that unauthorised third parties are denied access to LRZ's IT infrastructure, with this including, in particular, not using primitive, obvious passwords, changing passwords frequently and properly logging out at the end of a session;
d) report cases that might be relevant to security which he or she has gained knowledge of to the local person in charge of data processing or to the LRZ.

(4) The user bears full responsibility for all acts performed under his or her user account, even if these actions are performed by third parties that the user permitted to have access at least negligently. In this kind of case, the LRZ is authorised to demand the usage fees from the user that the third party would have had to pay in the case of regular usage.

(5) Furthermore, the user is obligated to

a) comply with the statutory regulations (legal protection of copyright, copyright) when using software (sources, objects), documentations and other data;

b) inform themselves regarding the terms under which the software, documentations or data were made available, partly within the framework of license agreements, and to observe these terms;

c) in particular, not copy software, documentations and data or pass them on to individuals other than those who are authorised to receive them, unless this is explicitly permitted, and, in particular, not use them for commercial purposes.

(6) Of course, the IT infrastructure may only be used in a legally appropriate manner. Attention is explicitly drawn to the fact that the following actions in particular are subject to legal prosecution according to the German Penal Code (StGB):

a) trying to find out other users' passwords, spying out and intercepting data (§ 202 a|b|c StGB)

b) unauthorised alteration, deletion, suppression or damaging of data to the point it can no longer be used (§ 303 a StGB)

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

d) dissemination of propaganda of unconstitutional organisations (§ 86 StGB) or depicting of violence (§ 131 StGB)

e) dissemination of certain forms of pornography on the Internet (§ 184 ff. StGB), in particular, accessing or ownership of documents containing child pornography (§ 184 (1) 5 StGB)

f) defamatory offences such as insults, libel or slander (§ 185 ff. StGB)

g) infringements of copyright, e.g. due to illegal duplication of software or offering of movies or pieces of music in a file sharing exchange (§ 106 ff. of the German Copyright Act, UrhG)

(7) Without the consent of the responsible system operator, the user is not allowed to

a) make changes to the hardware setup,

b) make changes to the configuration of the operating systems or the network.

The authorisation to install software is dealt with separately and is dependent on the respective local conditions or conditions in terms of system technology.

(8) Users are obligated to consult with the system operator prior to commencement of a project involving the processing of personal data. This shall be without prejudice to any obligations arising from the Bavarian Data Protection Act (Bayerisches Datenschutzgesetz).

(9) The user is not permitted to gain knowledge of and/or use certain messages intended for other users,

(10) The user is obligated to

a) observe the supplementary terms of use, regulations and guidelines for use provided by the system operator;

These include
- the regulations for the operation of the Munich Scientific Network (MWN)
- the regulations for the use of the archive system and backup system
- the guidelines on ethical and legal issues relating to the use of software
- the guidelines on the responsible use of data networks
- the code of use of the DFN Verein for the operation of the scientific network (DFN WiN)
- DEISA and EGEE Acceptable Use Policies.

b) abide by the usage and access regulations of other providers when communicating with their computers and networks.

§ 5 User liability

(1) The user is liable for all disadvantages resulting to the LRZ as a result of abusive or illegal use of LRZ's IT infrastructure and the authorisation of use or which result because the user did not comply with its obligations arising from the Usage Regulations.

(2) The user is also liable for damages resulting from authorised use by third parties if he or she is responsible for such use by a third party, e.g. because the user account was passed on. In this case, the LRZ is authorised to charge a usage fee for third party use in accordance with the catalogue of services.

(3) To the extent that the user can be held liable, he or she shall release the LRZ from any and all claims for damages, inaction or other relief brought against the LRZ by third parties as a result of the user's misuse or unlawful conduct. The LRZ will serve third party notice to the user in the event that third parties take the LRZ to court.

§ 6 The LRZ's rights and duties

(1) The LRZ shall document the user authorisations that have been issued insofar as it has not delegated this task to the designated individual for data processing or the Master User of an institution. In these cases, the designated individuals for data processing or Master Users are obligated to ensure proper documentation and safekeeping of the documents. The LRZ is authorised at any time to demand information on the user authorisations that have been issued along with the user status and to inspect the documentation. The papers and data that are prepared and provided in the course of an application or prolongation of a project at the LRZ along with the ensuing consumption data are saved by machine and are deleted immediately after the authorisation expires if they are no longer needed to carry out LRZ's duties. This does not apply to accounting data.

(2) Within the framework of the following provisions, the LRZ is authorised to document and analyse the use of the IT systems by the individual user, but only to the extent necessary:
   a) to guarantee 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 troubleshooting and
   f) for resolving and preventing unlawful and abusive use.

(3) The LRZ shall contribute to the prevention or detection of misuse in an appropriate manner, particularly in the form of regular audits. For this purpose, it is authorised in particular to check passwords and user data and to take the necessary measures in terms of protection, such as changing passwords that are easy to guess, in order to protect the IT infrastructure and user data from unauthorised access by third parties. If user passwords, access authorisations for user files and other protective measures relevant to usage need to be changed, the user shall be notified immediately.

(4) In order to guarantee proper system operation, the LRZ is also authorised to inspect user files, whilst observing data secrecy, insofar as this is necessary in order to eliminate existing faults or resolve and prevent acts of misuse. Inspection of the message and email boxes is only admissible insofar as this is indispensable for the elimination of existing faults in the message service. Inspection shall be documented in each case and the respective user shall be informed immediately after the goal has been achieved.

(5) The LRZ is obligated to maintain confidentiality.

(6) The LRZ shall designate a contact for organizational arrangements for the use of LRZ's services for all of the institutions with authorisations of use.

(7) The LRZ is obligated to abide by the usage and access guidelines of other providers when communicating with their computers and networks.

(8) For reasons of operation, the LRZ can restrict use of the IT infrastructure temporarily or block individual user accounts temporarily. The respective users shall be notified beforehand insofar as possible.

(9) If there are justified grounds that a user is making unlawful contents available on the LRZ's IT infrastructure, the LRZ may prevent further use until the facts of the case have been resolved sufficiently.

§ 7 The LRZ's liability

(1) The LRZ neither warrants that the system functions meet the user's specific requirements nor that the system will operate without fault or interruption. The LRZ cannot guarantee the integrity (with reference to destruction and manipulation) and confidentiality of the data stored in its IT system. Nonetheless, the LRZ shall make every effort to ensure a high level of quality of system and services.

(2) The LRZ shall not be liable for any damage whatsoever caused to the user resulting from the use of the LRZ's IT infrastructure, except for damage caused by intent or gross negligence of LRZ's employees or of the individuals employed to perform functions on LRZ's behalf.

§ 8 Miscellaneous

(1) Services that are subject to a fee for users of LRZ's IT infrastructure are described in the service catalogue of the Leibniz Supercomputing Centre ("Dienstleistungskatalog des Leibniz-Rechenzentrums") and may also be described in other fee codes.

(2) As necessary, supplementary or deviating usage regulations may be set up for specific systems. Due to regulations of the export authorities of the countries of manufacture, members or organisations of certain countries are not permitted to use parts of the IT infrastructure operated by the LRZ (§ 2, (1) a, b and d). Corresponding restrictions are listed in the documentation for accessing the respective systems.

(3) The Commission for Computer Science of the Bavarian Academy of Sciences and Humanities shall decide in the event of complaints by users if these cannot be settled by the Directorate of the Leibniz Supercomputing Centre.

(4) In the event that parts of these Usage Regulations are invalid or become so, such invalidity shall not affect the validity of the other parts.

(5) Munich shall be the place of jurisdiction for all legal claims arising from usage relationship.

§ 9 Final provisions

(1) Amendments of these regulations shall be decided by a simple majority of the Plenary Assembly in accordance with § 9 (5) sentence 1 of the Academy's articles of incorporation.

(2) These Usage Regulations shall enter into force after the adoption of the corresponding resolution on the day of publication on LRZ's homepage on the Internet.