

Technische Universität München

Acceptable Use Policy for Information Technology Resources

Last amended July 1st 2011

This translation of the document *Benutzungsrichtlinien für Informationsverarbeitungssysteme der Technischen Universität München* is provided for convenience only. If there is any contradiction between the German and English version, the German language version shall take precedence.

Introduction

Technische Universität München and its facilities ("Operator" or "System Operator") operate an IT infrastructure ("IT Resources") consisting of data processing systems (computers), communication systems (networks) and other information processing equipment.

The IT Resources are integrated into the *Münchener Hochschulnetz* network operated by the *Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ)*, the German National Research and Education Network (WiN), and the internet. For all services offered by LRZ such as network connection, e-mail, file storage, backup, archival and hosting, the LRZ guidelines shall apply in addition to this Acceptable Use Policy.

This Acceptable Use Policy sets out the conditions for the use of the Resources and applies to all persons accessing or using the Resources.

The Acceptable Use Policy

- is based on the statutory duties of universities and other institutions of higher education and their commitment to protecting academic freedom;
- sets out the general rules for proper operation of IT Resources;
- sets out the rights of third parties that must be complied with (e.g. software licenses, network provider requirements, data protection requirements);
- requires the user to adhere to a code of proper conduct and to make economical use of the Resources;
- sets out the Operator's rights and remedies in the case of violation of the Acceptable Use Policy.

Art. 1 Application

This Acceptable Use Policy shall apply to the IT infrastructure, i.e. the data processing systems (computers), communication systems (networks), services, applications and other information processing equipment (IT Resources), provided by Technische Universität München, its facilities and the LRZ.

Art. 2 Use of IT Resources

1. The IT Resources delineated in Art. 1 are provided to enable members of Technische Universität München to fulfil their responsibilities in the areas of research, teaching, administration, education/training, public relations, and corporate image of the university as well as other duties or responsibilities set out in Art. 2 of the Bayerisches Hochschulgesetz [Bavarian Higher Education Act].
2. Other individuals or facilities may be granted permission to use the IT Resources.
3. Members of the Technische Universität München must apply for their user authorization (see Art. 3 (1) with the organizational unit they are assigned to.

Art. 3 Formal User Authorization

1. Use of IT Resources pursuant to Art. 1 requires formal user authorization by the System Operator, except for services configured for anonymous access (e.g. information services, library services, temporary guest permits for conferences).
2. The organizational units within the Technische Universität München, including, but not limited to, its academic departments, institutes, operational units, Lehrstühle, and other entities, shall be the System Operators of their respective systems.
3. The application for formal authorization shall include the following information:
 - a. Operator/institute or organizational unit to which applications must be submitted;
 - b. description of the systems for which user authorization is requested;
 - c. applicant: name, address, phone number (students must indicate their student ID number) and, if applicable, data for use in information services and affiliation with an organizational unit of the university;
 - d. general information on the intended use of the IT Resources, e.g. research, education/training, administration;
 - e. user's consent authorizing Operator to change user authorization and user data (e.g. password) to protect system operation. User must be informed of any change without delay;
 - f. user's acceptance of the Acceptable Use Policy, either in writing or in digital form. Users must actively declare their acceptance by checking the relevant box in the application documents (opt-in acceptance).
4. All relevant data protection requirements must be complied with. Operator may not request additional information unless it is required for the decision on the application. The application will be decided by the responsible System Operator. The System Operator may make the granting of the user authorization dependent upon evidence of a certain level of competence in using the system concerned.
5. User authorization may be denied if
 - a. it seems uncertain that the applicant will fulfil his/her obligations as a user;
 - b. the free capacity of the system for which authorization is being requested is not sufficient for the intended use;
 - c. the intended use is not in compliance with the purposes delineated in Art. 2 (1) and 4 (1);
 - d. the system is obviously not suitable for the intended use, or is reserved for a special purpose;
 - e. the system for which authorization is requested is connected to a network that is subject to special data protection requirements and there are no objective grounds for the access request;
 - f. it is to be expected that the requested use would unreasonably disturb other authorized uses.
6. The User Authorization shall be limited to activities related to the requested use.

Art. 4 User Responsibilities

1. IT Resources as defined in Art. 1 may be used only for the purposes set out in Art. 2 (1). Any use of the IT Resources for other purposes, in particular economic purposes, is granted only upon request and in return for a fee.
2. Users shall exercise due diligence in using the resources (work stations, CPU capacity, disc space, line capacity, peripheral devices, and consumables) responsibly and economically. Moreover, 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 Resources and/or other users. Non-compliance with this Policy may lead to claims for damages (Art. 7).
3. Users shall refrain from any misuse of the IT Resources. In particular, Users are obligated
 - a. to use only their officially assigned User ID; transfer or sharing of User IDs and passwords is not permitted;
 - b. to protect access to IT Resources by a user-defined confidential password or a similar security measure;
 - c. to exercise due diligence to prevent unauthorized persons from access to IT Resources; this includes, but is not limited to, not using primitive, obvious passwords, changing the passwords more frequently, and logging out appropriately at the end of each session. Within the statutory requirements, Users shall be responsible for all actions taken under their User ID, even if these actions were taken by third parties to whom User has provided access, provided that this was caused by culpable conduct on the part of User.

Further, Users are obligated

- d. to abide by the statutory provisions (copyright protection) when using software (sources, objects), documentations and other data;
- e. to make themselves acquainted with the provisions of any license agreements governing software, documentations and/or data, and to abide by such provisions;
- f. neither to copy or distribute software, documentations and data etc., unless explicitly permitted, nor to use them for any purposes other than the permitted purposes, in particular not to use them for commercial purposes.

Non-compliance with this Policy may lead to claims for damages (Art. 7).

4. As a matter of course, IT Resources may be used only for legitimate, legal activities. Users are expressly advised that misconduct, including, but not limited to the actions stated below, is an offence under German criminal law:
 - a. password spying, data espionage (§ 202 a StGB [German Criminal Code]);
 - b. data tampering, i.e. unlawfully altering, deleting, or suppressing data or rendering data unusable (§ 303 a StGB);
 - c. computer sabotage (§ 303 b StGB) and computer fraud (§ 263 a StGB);
 - d. dissemination of propaganda material of unconstitutional organizations (§ 86 StGB) or dissemination of racist ideas (§ 131 StGB);
 - e. distribution of certain types of pornography on the internet (§ 184 Abs. 3 StGB);
 - f. accessing, downloading or storing of material containing child pornography (§ 184 Abs. 5 StGB);
 - g. defamation, insult, libel, slander (§ 185 et seq. StGB);

System Operator reserves the right to institute criminal or civil proceedings (Art. 7).

5. Without prior approval of the responsible Operator, User shall not have the right to
 - a. make changes to the hardware setup;
 - b. modify the system software or network configuration.

Separate provisions apply to the authorization to install software, depending on local and system requirements.

6. Users are obligated to consult with 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 Bayerisches Datenschutzgesetz [Bavarian Data Protection Act].

Users are not permitted to access and/or process certain data and messages on behalf of other users.

7. Users are obligated
 - a. to comply with any supplemental terms of use, policies, and guidelines provided by System Operator;
 - b. in interactions with computers and networks of other users, to respect their terms of access and use.

Art. 5 System Operator's Tasks, Rights and Responsibilities

1. System Operators must document all user authorizations granted. The documentation must be stored for a minimum period of two years from expiry of each authorization.
2. System Operator will appropriately contribute to preventing or detecting misuse of IT Resources. For this purpose, Operator shall be entitled to take any of the following actions, in particular
 - a. to check password and user data security and take protective measures, e.g. change or disable easily guessable passwords to protect them from unauthorized access. User must be notified accordingly without delay;
 - b. to document and evaluate user activities provided that this serves the following purposes: accounting, resource planning, protection of personal data of other users, operation monitoring and/or identification of errors and violations of the Acceptable Use Policy and/or statutory regulations;
 - c. in case of suspected violation of the Acceptable Use Policy or conduct in violation of criminal law, to inspect user files or mailboxes or to record details of a User's network usage, for example by means of a network sniffer, in compliance with the four-eye principle and the applicable recording requirements (for TUM employees, the provisions of the *Rahmendienstvereinbarung zur Verarbeitung systemimmanenter Daten, des Einsatzes von Fernüberwachungsmaßnahmen und der Einsichtnahme in Benutzerdaten an der Technischen Universität München* shall apply); the inspection must be documented and the User concerned must be informed without delay upon achievement of the purpose;
 - d. to take measures to secure evidence, such as keystroke logging or network sniffers, in the event there is reasonable suspicion of a criminal offence.
3. System Operator shall maintain confidentiality.
4. System Operator will identify the staff responsible for IT support.
5. In any interactions with computers and networks of other users, System Operator shall respect the terms of access and use of the other users.
6. For operational reasons, Operator may restrict the use of the IT Resources or disable certain User IDs temporarily. If possible, the Users concerned shall be notified in advance.
7. If there are actual indications that a User makes unlawful content available for use through IT Resources, Operator may prevent User from using the IT Resources until the legal situation is adequately resolved.

Art. 6 System Operator's Liability; Disclaimer

1. System Operator neither warrants that the system functions meet a User's specific requirements nor that the system will operate without fault or interruption. Further, System Operator cannot guarantee the integrity (protection from destruction and manipulation) and confidentiality of the data stored in its IT systems.
2. System Operator shall not be liable for any damage whatsoever caused to User resulting from the use of IT Resources specified in Art. 1, except for damage caused by intent or gross

negligence of System Operator or those persons employed to perform functions on behalf of System Operator.

Art. 7 User's Liability

1. Users, within the statutory requirements, shall be liable for any damage or loss caused to System Operator as a result of misuse or unlawful use of IT Resources or user authorization or User's culpable non-compliance with the obligations stipulated in this Policy.
2. Within the scope of access and use supported by his/her user authorization, User shall also be liable for any damage caused by third parties if User is responsible for the third-party use, in particular as a result of transferring or sharing his/her User ID to/with third parties. In such a case, the System Operator may require the User to pay a fee for the third party use.
3. To the extent User can be held liable, User shall release System Operator from any and all claims for damages, injunctive or other relief brought by third parties against System Operator as a result of User's misuse or unlawful conduct. Should proceedings be brought against System Operator by a third party, System Operator will serve a third-party notice upon User.

Art. 8 Consequences of Misuse or Illegal Use

1. In the event of violation of the law, this Acceptable Use Policy, in particular Art. 4 (User Responsibilities), or in the event that System Operator suffers any harm as a result of other unlawful actions of User, System Operator may restrict or withdraw the user authorization as a whole or in part irrespective of whether or not the violation has caused damage.
2. In the event of serious or repeated violations, User may be permanently banned from using the IT Resources specified in Art. 1.
3. The User concerned will be given the opportunity to comment on the matter and to save his/her data.
4. Any violations of the law, labour law, public sector employment law, or the provisions of this Acceptable Use Policy will be investigated in terms of criminal or civil liability. Violations deemed significant will be referred to the competent legal department to decide whether further steps need to be taken. System Operator expressly reserves the right to institute criminal or civil proceedings.

Art. 9 Miscellaneous

1. Separate policies may stipulate that the use of IT Resources is subject to a fee.
2. Supplemental or different policies may apply to certain systems, if required.
3. For employees, supplemental or different policies may apply as set forth in employment contracts, public sector employment and/or collective bargaining law provisions.
4. If any provisions of this Acceptable Use Policy for Information Technology Resources should be or become invalid, this shall not affect the validity of the remaining provisions.
5. Venue for all litigation arising out of or in connection with this Acceptable Use Policy shall be Munich, Germany.

Art. 10 Entry into Force

This Acceptable Use Policy for Information Technology Resources shall enter into full force and effect on the day after its promulgation.

Munich, July 1st 2011

Herbert Vogg

Leiter IT-Servicezentrum