Terms of Use for IT Systems of the Technical University of Darmstadt

–Translation help, the German version is binding–
Information Security TU Darmstadt
Published: October 1, 2019 (original German version)

TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec
TU Darmstadt

Based on the approval of the Executive Board of the Technical University of Darmstadt dated 01.10.2019, the User Regulations for IT Systems of the Technical University of Darmstadt, are published below.

Darmstadt, 01.10.2019

The President of the Technical University of Darmstadt

Prof. Dr. Tanja Brühl

Terms of Use for IT Systems of the TU Darmstadt

Contents

Preamble

The University, its departments and facilities operate an information technology (IT) infrastructure consisting of physical and virtual information processing systems and a multiservice communication network for the transmission of data, images and speech. This IT infrastructure is connected to the worldwide Internet.

The present terms of use regulate the conditions under which the services offered by this infrastructure may be used; it

- establishes basic rules for proper operation of the IT infrastructure.
- obligates operators to operate the systems correctly and to comply with IT security standards in accordance with the hessian information security guidelines.
- points out the rights of third parties that must be protected (e.g. with regard to software licenses, the requirements of network operators or data protection aspects).
- obliges users to behave correctly and to use the resources offered economically.
- is guided by the legally defined tasks of the university as well as its mandate to preserve academic freedom.
- informs about possible measures in case of violation of these terms of use.
- obligates the respective managers to ensure that users and operators have the necessary expertise in their area of responsibility.

§ 1 Area of application

- These terms of use apply to the IT infrastructure operated by the Technische Universität (TU) Darmstadt, consisting of information processing systems, communication systems and other auxiliary equipment as well as the commissioning of subcontractors in the area of IT infrastructure.
- In order to maintain the proper operation of the IT infrastructure and services, the management of the respective organizational units may define further specific regulations and guidelines for the individual services. These are to be documented and made available to the affected users in an adequate manner.
- These terms of use are binding for all users and operators of the IT infrastructure of the TU Darmstadt.

§ 2 Users and tasks

1. The IT resources specified in § 1 are available to the members of the TU Darmstadt for the fulfillment of their tasks from research, teaching, studies, transfer, administration, education and training and public relations within the framework of the TU Darmstadt.
2. Other persons and institutions may be permitted to use the systems, provided that they commit to complying with the terms of use, the data protection regulations and the applicable rules.

§ 3 Authorizations of use

1. In order to use the IT resources according to § 1, a formal authorization of use - e.g. user ID, network connection, network access - from the respective responsible system operator[1] is usually required. Passwords must at least comply with the password guideline of the University Computing Centre (Hochschulrechenzentrum, HRZ)[2].

[1] In this document, system operator means the organizational unit that operates IT systems or has them operated.
[2] The reference to the guidelines of the HRZ originates from 2019. With the establishment of the Information Security Department, the central information security regulations apply for all information security related aspects, e.g., the current password policy.

2. All computers operated on the TU Darmstadt network must be registered with the HRZ. As a rule, computers can only be registered by employees of the TU Darmstadt via their respective domain representatives. In the case of student groups, members of the TU Darmstadt can perform the registration. Substitutes ensure the accessibility. These persons provide information about rights and obligations and collect the required data and forward them to the HRZ.
3. The application for a formal authorization of use shall include the following information:
    a) System operator from whom the authorization of use is requested;
    b) Systems for which the authorization of use is requested;
    c) Applicant: Name, address, telephone and/or fax number and, if available, e-mail address (for students also matriculation number) as well as affiliation to an organizational unit of the university;
    d) Information on the purpose of use, e.g. research, training/teaching, administration;
    e) the declaration that the user acknowledges these terms of use and consents to the collection and processing of his/her own personal data for the purpose of user administration, in particular in accordance with § 8 number 6, 7, 8 of these terms of use. Obligation to comply with the terms of use, data protection regulations and applicable rules.
4. The system operator may request further information only to the extent that it is necessary for the decision on the application or the system operation. The responsible system operator decides on the application. The system operator may make granting of the authorization dependent on the proof of certain knowledge about the use of the system.
5. The granting of the authorization of use may be refused if
    a) the intended use is not compatible with the purposes according to § 2 of these terms of use;
    b) there is no guarantee that the applicant will fulfill his/her obligations as a user;
    c) the system is obviously unsuitable for the intended use or reserved for special purposes;
    d) there are reasonable doubts based on concrete indications that the intended use will unreasonably interfere with other authorized uses;
    e) the required IT resources are connected to IT infrastructures that must meet special data protection requirements and no objective reason for the intended use is apparent;
    f) reasons of foreign trade law do not permit use by citizens of certain countries.
6. The authorization of use only entitles the user to use the system for tasks in accordance with the application.

§ 4 Legal involvement and guidelines

The IT infrastructure may only be used in a legally correct manner. It is expressly pointed out that the following activities are punishable under the Criminal Code:

a) spying out data, in particular the unauthorized obtaining of data of others that are specially secured against unauthorized access (Sections 202a, 274 (1) No. 2 StGB);

b) falsely influencing data processing (§§ 270, 269 StGB), unlawfully deleting, suppressing, rendering unusable or altering data (§ 303a StGB);

c) computer sabotage (§ 303b StGB) and computer fraud by incorrect design of a program, by using incorrect or incomplete data, by unauthorized use of data or by unauthorized interference with the process (§ 263a StGB);

d) the dissemination of propaganda material of unconstitutional organizations (§ 86 StGB) or racist ideas (§ 130 StGB);

e) offering or providing pornographic writings (§ 184 Abs. 1, Ziffer 3 StGB);

f) retrieval or possession of documents containing child pornography (§ 184 Abs. 1, Ziffer 5 StGB);

g) honor crimes such as insult or defamation (§ 185 ff StGB), insults to confessions, religions or world views (§ 166 StGB);

h) copyright infringements, e.g. by copying software in violation of copyright law or entering protected works into a data processing (DP) system (§§ 106 et seq. UrhG);

i) the violation of private secrets (§ 203 StGB);

j) the violation of telecommunications secrets (§ 206 StGB);

k) destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier (§ 303b StGB);

l) the use of personal data contrary to the provisions of the HDSG (§ 40 HDSG);

m) Employees who endanger the security of data, information, ITC systems or the network and cause damage to the TU Darmstadt or the State of Hesse or a third party may be required to pay compensation (§ 48 BeamtStG, § 3 para. 7 TV-H, § 823 BGB) or be subject to a recourse claim (Art. 34 GG in conjunction with § 839 BGB).

In some cases, even the attempt is punishable.

When processing personal data, users and operators must inform themselves about the relevant data protection regulations in order to comply with the European Data Protection Regulation (EU-DSGVO) and the Hessian Data Protection and Freedom of Information Act (HDSIG).

When using IT infrastructure, users and operators must inform themselves about and comply with the information security guidelines of the state and the information security guidelines of the TU Darmstadt.

§ 5 Duties of the users

1. The IT resources according to § 1 may only be used for the purposes specified in § 2 number 1 of these terms of use. Any use deviating from this requires separate approval.
2. Users are obliged to ensure that they use the available operating resources (e.g. workstations, CPU capacity, storage space, line capacities, peripheral devices and consumables) responsibly and economically. The user is obligated to refrain from impairments of the operation, as far as they are foreseeable, and to avoid everything to the best of his/her knowledge that could cause damage to the IT infrastructure or to other users. Violations may result in claims for damages and exclusion from use (see also § 11 of these terms of use).
3. The user must refrain from any kind of misuse of the IT infrastructure. In particular, he/she is obliged to,
   a) work exclusively with user authorizations that he/she has been provided with; passing on a user ID together with the associated secret password is not permitted. The unauthorized passing on of electronic access mechanisms (chip card) is generally not permitted;
   b) take precautions to prevent unauthorized third parties from accessing IT resources; this includes, in particular, avoiding obvious passwords (see the design guideline of the TU Darmstadt's password policy), changing passwords more frequently, and logging out or locking the workstation when leaving it.
   c) not to determine or use third-party user IDs and passwords;
   d) not to gain unauthorized access to information of other users and not to pass on, use or change information of other users without permission;
   e) inform the system operators if he/she becomes aware of the misuse of his/her own user ID.

   The user is fully responsible for all actions performed under his/her user ID, even if these actions are performed by third parties to whom he/she has at least negligently provided access.

   The user is furthermore obliged to,

f) comply with the legal regulations (copyright protection, copyright, etc.) when using software (sources, objects), documentation and other data;

g) inform her/himself about the conditions under which the software, documentation or data acquired in part under license agreements are made available and to observe these conditions;

h) in particular software, documentation and data, unless expressly permitted, neither to copy nor to pass them on nor to use them for purposes other than those permitted, in particular not for commercial purposes.

Violations may give rise to claims for damages (§ 11).

4. The user is obligated to coordinate any plans to process personal data with the company's data protection officer and to create and maintain appropriate data protection documentation. The data security precautions specified by data protection officers and, where applicable, system operators must be complied with.

5. The user is obliged to,
   a) observe the guides for use provided by the system operator;
   b) provide the person responsible for the system with information about programs and methods used for control purposes in justified individual cases - in particular in the event of justified suspicion of misuse and for troubleshooting. This provision does not cover usage data protected by telecommunications secrecy or data secrecy, e.g. personal data of third parties;
   c) inform himself about the respective local and system technical conditions and regulations before installing software and to follow them.

6. The user as a provider of information on the World-Wide Web (WWW)
   a) bears the responsibility for the content of his/her WWW pages;
   b) must indicate the imprint on each WWW page, which shows the person responsible for the page and the corresponding contact information;
   c) must provide a privacy statement on each WWW page.
   The TU Darmstadt provides corresponding templates for its central web offerings.

7. The user is obligated to regularly use the university e-mail address assigned to him/her in order to obtain knowledge of administrative communications from the university.

8. IT security incidents and emergencies of any kind must be reported to cert@.tu-darmstadt.de[3] or by calling the TU internal number 27777. The members of the TU Darmstadt Computer Emergency Response Team (TUDa-CERT) are appointed by the Executive Board. The instructions of the TUDa-CERT members must be followed in the event of an IT security incident or emergency.

§ 6 Liability of the users

1. The user is liable for all disadvantages incurred by the university due to misuse or illegal use of the IT resources and usage authorization or due to the user's culpable failure to comply with his/her obligations under these terms of use. The University may demand that misused resources and any further costs arising therefrom be reimbursed.

2. The user is also liable for damages caused by third party use within the scope of the access and use options made available to him/her, if he/she is responsible for this third party use, in particular in the event of his/her user ID being passed on to third parties.

3. The user shall indemnify the University against all claims if third parties assert claims for damages, injunctive relief or other claims against the University due to abusive or unlawful conduct on the part of the user.

[3] The original document states security@hrz.tu-darmstadt.de as contact address, which is outdated.

§ 7 End of the usage relationship

1. The admission to use ends with the loss of the status (§ 2) or cessation of the reasons on the basis of which the admission was made.
2. The HRZ uses an automated system for identity management to manage and organize the affiliation of members and relatives of the TU Darmstadt and other authorized users as defined in § 2.
3. The operator can store the user's data for up to six months and then delete it, provided that this does not conflict with official or legal interests or other agreements.

   The obligations of the users under service and employment law after the end of the usage relationship with regard to data transfer and data backup and the requirements of the guidelines for handling digital research data at the TU Darmstadt in the currently valid version remain unaffected.

§ 8 Tasks, rights and obligations of system operators

1. The system operator may keep a file of the users with the personal data of the users about the granted user authorizations. For this purpose, a register of processing activities (VVT) must be created and maintained.
2. The system operator shall disclose the system responsible person(s) for the support of its systems. The system operator and the system responsible persons are obliged to maintain confidentiality.
3. The system operator may temporarily restrict the use of its resources or temporarily block individual user IDs, insofar as this is necessary for troubleshooting, system administration and expansion, or for reasons of system security and the protection of usage data. If possible, the affected users are to be informed immediately.
4. If there are reasonable indications to believe that users are providing illegal content on the system operator's servers, the system operator may prevent further use until the legal situation has been adequately clarified.
5. As a rule, access to IT resources must be protected, e.g., by means of a password to be kept secret, chip card or an equivalent procedure.
6. The system operator is entitled to check the security of passwords and usage data by regular manual or automated measures and to initiate necessary protective measures, e.g., changes of easily guessed or outdated passwords, in order to protect the data processing resources and usage data from unauthorized access by third parties. The user must be informed immediately of any necessary changes to passwords, access rights to usage data and other protective measures relevant to usage.
7. The system operator is entitled to document and evaluate the use of the data processing systems by the individual users for the following purposes:

   a) to ensure 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 the detection and elimination of malfunctions as well as
   f) for the clarification and prevention of illegal or improper use.

   For this purpose, a register of processing activities (VVT) must be created and maintained.
8. The system operator is also entitled to inspect the files of the users, insofar as this is necessary for the elimination of current malfunctions or for the clarification and prevention of violations of the terms of use and if there are indications for this. The data secrecy is to be observed.

   In any case, the inspection must be documented, and affected users must be notified immediately after the inspection has taken place, as soon as this is possible after the purpose has been achieved.

In the event of justified indications of criminal acts, the system operator will act in consultation with the university management in consultation with the relevant authorities and will – if necessary – use evidence-protection measures.

9. System operators who offer users independent home pages for publication on the Internet are entitled to automatically generate an imprint on these pages that contains the full name and e-mail address of the authors.

10. In accordance with the statutory provisions, the system operator is obliged to maintain telecommunications and data secrecy.

11. The correct licensing of the software used in his/her area of responsibility is the responsibility of the system operators. This also includes maintaining the necessary documentation and providing users with sufficient information about the framework conditions to be observed.

12. System operators appoint contact persons for their systems and report at least one contact person per area to the IT security officers at TU Darmstadt.

13. IT security incidents and emergencies of any kind are reportable at cert@tu-darmstadt.de or via telephone 27777. The system operator is responsible for ensuring that this notification is made by the users themselves or by the system operator. The members of the TU Darmstadt Computer Emergency Response Team (TUDa-CERT) are appointed by the Executive Board. The instructions of the TUDa-CERT members must be followed in the event of an IT security incident or emergency. In addition, operators shall provide the IT security officers with all requested information necessary for reporting to higher-level authorities.

§ 9 IT Security

The management of a TU organizational unit bears responsibility for appropriate information security in the area for which it is responsible in accordance with the information security guidelines of the state and the information security guidelines of the TU Darmstadt.

1. In consideration of the value of the information to be protected, the risks as well as the expenditure of personnel and financial resources for information security, an appropriate level of information security is to be strived for and achieved for IT systems used and planned at the TU Darmstadt. For IT systems with a normal need for protection, security measures – based on the BSI's basic protection standards and basic protection catalogs as well as the international standards DIN ISO/IEC 27001 ff. – must be provided for and implemented. For areas where a higher need for protection is identified, supplementary security measures must be introduced and documented.

2. The management of a TU organizational facility is responsible for ensuring that security measures are implemented in the area for which it is responsible. Within the scope of their respective possibilities, employees should avoid internal and external security incidents and report security-relevant incidents to the responsible persons immediately so that corrective measures can be initiated as quickly as possible. In each TU organizational unit, a contact person is appointed for the IT security officer, who provides the necessary information for the respective protection requirement and takes the appropriate security measures in each case, taking into account affordability and cost-effectiveness.

§ 10 Liability of the network operator/exclusion of liability

1. The system operator does not guarantee that the system functions meet the specific requirements of the users or that the system runs error-free and without interruption. The TU Darmstadt does not guarantee the integrity (in terms of destruction, manipulation) and confidentiality of the data stored by it.

2. The system operator is not liable for damages of any kind incurred by the user as a result of the use of the IT resources in accordance with § 1 of these terms of use, unless otherwise stipulated by mandatory legal provisions.

§ 11 Consequences of improper or unlawful use

In the event of violations of statutory provisions or of the provisions of these terms of use, in particular of § 5 (Rights and Duties of Users), the system operator may restrict the authorization of use. It is irrelevant whether the violation resulted in material damage or not.

Measures to withdraw or restrict the authorization of use, which are decided by the management of the facility, should only be taken after a prior unsuccessful warning. The person concerned must be given the opportunity to comment.

§ 12 Employees as operators and users

Employees of the TU Darmstadt are obligated to exercise particular care in the operation and use of the IT systems of the TU Darmstadt. With regard to the employer's duty of care and the duty of care of the responsible managers, the following additional regulations apply:

1. The laws and guidelines cited in § 4, § 5 number 3f, § 5 number 5a shall be made available to employees in an appropriate manner.
2. The employees are informed in an appropriate manner about
   a) responsible and economically reasonable use and the duty to avoid damage (§ 5, item 2);
   b) the conditions under which software, documentation or data, some of which are acquired under license agreements, are made available (§ 5 number 3g), provided that these entail certain rules of conduct in the official context;
   c) the handling of personal data within the framework of projects for the processing of such data (§ 5 number 4);
   d) the standards in the context of publishing information on the World-Wide-Web (WWW) (§ 5, item 6 and § 11a, item 3).
3. The provider of information on the World-Wide-Web (WWW) (§ 5, clause 6) is the President of the TU Darmstadt. With regard to the contents, the employees are obligated to coordinate with all responsible offices of the TU Darmstadt and to be particularly sensitive when dealing with posted information. With regard to the imprint and privacy policy, the standards specified for this apply.
4. Employees of the TU Darmstadt are subject to the liability privileges under labor and employment law, according to which they are liable for intent and gross negligence.
5. The system operator is only permitted to view the files of the users if this is necessary to eliminate current malfunctions or to clarify and prevent violations of the terms of use and if there are indications for this. As a rule, the inspection is carried out in coordination with the personnel manager of the area in which an inspection is required. Only if this is necessary to avert danger, information will be provided as soon as this is necessary within the scope of achieving the purpose.
6. The respective managers shall ensure that their employees have the necessary expertise to comply with these terms of use and thus to operate and use the IT infrastructure of the TU Darmstadt. The TU Darmstadt offers suitable training events.

§ 13 Other regulations

1. Charges or fees may be set for the use of IT resources. The fee schedule of the respective system operator shall apply.

2. If necessary, supplementary or deviating rules of use may be specified for individual systems. Supplements to or deviations from § 12 require the involvement of the Staff Council of the TU Darmstadt insofar as regulations are concerned which affect employees who are represented by the Staff Council in accordance with § 3 and § 97 of the Hessian Staff Representation Act.

3. The responsible university management decides on changes to these terms of use.

§ 14 Coming into Effect

These terms of use shall come into effect on the day following publication in the Statutes Supplement of the Technical University of Darmstadt. The ” Allgemeine Benutzungsordnung für die Informationsverarbeitungs- und Kommunikations-Infrastruktur” (General Regulations for the Use of the Information Processing and Communications Infrastructure) of March 13, 2000, published in the Hessischer Staatsanzeiger 17/2000, shall cease to be in force when these regulations come into effect.

Darmstadt, 01. October 2019

Prof. Dr. Tanja Brühl
The President of the
Technical University of Darmstadt