# User rules of the IT departments of the “Trier University of Applied Sciences”

## Introduction

The IT departments of the „Trier University of Applied Sciences“ are operating the university-wide IT-infrastructure for studies, research, and administration. The facilities, IT-systems, data networks, and services are available for every member of the “Trier University of Applied Sciences” in accordance with the available capacities. The user rules ensure an error-free, unimpeded, and safe usage of the entire, centrally maintained IT-infrastructure of the “Trier University of Applied Sciences”. The user rules are guided by the duties and services defined in the organizational rules for the IT departments. The user rules maintain basic rules for the proper operation of the IT-infrastructure. Furthermore, they clarify the relationship between the user and the IT department. In case of questions, suggestions, or complaints, the user has the possibility to contact service members or the management of the IT department at any time.

## §1 Definitions of terms

1. Words indicating one gender include all genders.
2. The IT departments of the “Trier University of Applied Sciences” are facilities belonging to the “Trier University of Applied Sciences” under the responsibility of the president. The organizational regulations of the IT departments in its current terms of 29.04.2015 require in §3, article 2 the details of usage to be regulated by user rules.
3. The IT departments perform publicly accessible and licensing requiring services. The usage of a service that requires licensing is defined as the utilization of the IT department, the person who uses a service is defined as the user. The usage of services being accessible publicly does not apply as utilization within the meaning of these user rules.

## §2 Authorized users

Eligible for authorization as a user of the IT departments are:

1. Members according to §36 HochSchG as well as honorary professors, lecturers, and scientific assistants (§§ 62 – 64) while performing job-related tasks or during their studies,
2. members and facilities of other state universities/schools or state funded research institutes, based on existing agreements with “Trier University of Applied Sciences”,
3. any other natural or legal persons, who, as guests or co-operation partners of "Trier University of Applied Sciences", use IT resources or services within capacities which are not exhausted by the users according to (1) and (2).

## §3 Authorization

1. The utilization of access restricted IT-services provided by the IT departments happens by the allocation of an individual user-ID, which will be provided by the IT departments.
2. Students, as well as employees of the “Trier University of Applied Sciences” automatically receive a user-ID at the beginning of their studies or their recruitment. The user is fully responsible for any use of services made through his account.
3. For students the usage authorization ends with the de-registration. The account will be deactivated after the user has been contacted by personnel of the IT department and given some time as a grace period.
4. For employees of the “Trier University of Applied Sciences” the usage authorization ends when the employment relationship has ended. Decisions about further usage of business data will be made by the responsible supervisor.
5. Other users, applying for special agreements, such as above-mentioned (§2, article 3) receive an authorization which is generally temporary and based on the existing agreement with the “Trier University of Applied Sciences”. In case of extension or reduction of the employment, the responsible IT department has to be informed immediately.
6. Students receive the information about their user authorization along with their enrolment certificate in the mail or can pick it up at the student registration office. Due to privacy guidelines, employees will be handed out their information about their user authorization including user-ID, personal password, and the receipt of these user rules, only in person and on receipt of a written confirmation.

## §4 Access to workspaces of the IT departments

1. The workspaces of the IT departments are open for publicly accessible during general opening hours and office hours.
2. Arrangements for access to the workplaces out of the general opening hours will be released on the website of the particular IT department.
3. You are to recognize and follow the opening and office hours published by the IT departments.
4. If using workspaces of the IT departments out of office hours, instructions given by the personnel of the security company have to be followed.
5. Before using a single computer or whole workspace of the IT department, eventual reservations of workspaces for courses have to be checked and respected. Corresponding notices are located at the entrances to the workspaces.

## §5
## Terms of use

With the receipt of a user-ID the user undertakes:

a) to acquire the necessary skills to be able to use the IT-systems and services offered by the IT departments correctly;

b) to follow the terms of use and to not obstruct or affect other users while using the available workspaces of the IT departments;

c) to use the given user-ID exclusively for himself/herself in accordance to work-related purposes or studies for the "Trier University of Applied Sciences" and/or cooperating organisations and institutions;

d) to prevent potential abuse of his or her use-ID, more particularly not to share the own password with third parties and to choose an appropriate password, which is not easy to be guessed;

e) to protect personal programs and data of abuse by making use of the defence mechanisms of the particular system;

f) to ensure either by oneself or with help of a responsible supervisor that every used computer within the IT department is updated to the latest available version of the particularly used system, including an activated and constantly updated virus protection as well as all security-related updates and patches being installed;

g) to appropriately use every issued device, system, medium, or facility within the IT departments and to leave the workspace clean and organised;

h) to treat other users with respect and to treat the available resources of the IT department with consciousness;

i) to immediately report any issues, damages and problems with any device, system, medium, or facility within the IT departments;

j) to follow instructions of the responsible employees of the IT departments while using the workspaces and facilities;

k) to follow the terms of use while using software, documentaries, and other data, being under legal requirements, especially copyright and data protection and to respect license terms and conditions under which software, documentaries, and other data are released by the IT department;

l) to coordinate intentions of editing personal data with the responsible system operator beforehand. Excluding obligations occurring as a result of the regulations of the data protection law;

m) to follow the applicable law, especially applicable terms of the criminal law;

n) not to disturb courses taking place in the workspaces of the IT departments or impede them by blocking resources (cf. §4 bullet number 5);

o) not to install third-party software on any computer of the IT department without approval of the responsible supervisor;

p) to never access services offered by the IT department by using another user-ID besides the user-ID uniquely assigned to him or her;

q) not to attempt to gain unauthorised access to protected, encrypted or not publicly accessible data;

r) not to use protected, encrypted or not publicly accessible data, to which he or she accidently gained access to, neither for him or herself, nor to pass it on (for example transferring licensed software to a personal computer)

s) not to attempt any repair work on its own due to any issues, damages and problems with any device, system, medium, or facility within the IT departments;

t) not to eat, drink (excludes clear water), or smoke while staying in the facilities or making use of workspaces provided by the IT department.

It is explicitly pointed out that the following behaviours will lead to punishment in accordance to the criminal law:

a) Spying out other passwords or personal data (§202 StGB);

b) Unauthorised changing, deleting, supressing, or disabling of data (§303 StGB);

c) Computer sabotage (§303 StGB) or computer fraud (§263 StGB)

d) Promoting the distribution of propaganda of unconstitutional organisations (§86 StGB) or racist ideas (§131 StGB);

e) Spreading or receiving documents of pornographic content (§184, article 3 and article 5 StGB);

f) Receiving or being in possession of documents including child pornography (§184, article 5 StGB);

g) Defamation like libel or slander (§§ 185 ff. StGB).

## §6
## IT-network usage

1. Access to the computer network:

a) Every member of the "Trier University of Applied Sciences" is eligible to demand an IT-device, being used for work-related tasks or studies as well as research and administration, getting connected to the IT-network of the "Trier University of Applied Sciences". The connection of this device will be performed by the IT departments based on available possibilities and the state-of-the-art standards.

b) In case of the device not being administrated by the IT departments, the user has to take care that the device that is getting connected has all required hardware, software and security systems installed. The IT departments give recommendations and help in the selection of appropriate components.

c) The administrative data received with the connection (such as IP-address, computer name, network masks…) of a terminal device are to be treated as the user identification. In particular, the administrative data is only to be changed upon approval by the IT departments.

2. Network operation:

a) In accordance with state-of-the-art technology, the administrator of a terminal device has to guarantee that the connection of the device to the network can´t cause danger or damage to other network participants or devices connected to the network. The user is obliged to keep the security software as well as anti-virus software up to date at any time.

b) The provider of a terminal device has to ensure that only authorized individuals make use of the network services available through the device and that they follow these user rules. Necessary arrangements have to be made to be able to prove if and when other individuals besides the provides made use of network services using the terminal device.

c) The IT departments are entitled to temporary shutdown network components or remove devices from the network in consultation with the users to do tests and maintenance and conduct troubleshooting.

d) Preserving integrity is the users' responsibility. The IT departments take no responsibility for the accuracy of the transferred data.

e) For the joint use of networks, the respective applicable regulations and rules have to be followed.

## §7
## Rights and obligations of the IT departments

1. The IT departments have the right:

a) to operate security systems (such as alarm systems, video recording, entrance control) in order to keep the systems, devices and facilities safe and analyse personal data and information in case of damage. Possible involvement of staff council happens according to existing service agreements;

b) to check on and analyse data and programs of the users for test purposes if company interests are touched (e.g. in case of operations disruption or reasonable suspicion of misuse), in accordance with the data protection laws;

c) to save personal data that are required in order to issue a user-ID or to offer IT-services (cf. §3, article 2 and 3)

d) to publish name, surname, field of study/department and Email-address of a user by using electronic information systems;

e) to ask users for their work, utilized programs and methods;

f) to release further user rules as well as temporary priorities or set restrictions in order to ensure optimal securing of the services offered by the IT departments;

g) to temporary put certain IT-services out of operation due to test purposes or technical changes and improvements

h) to withdraw the user-ID and usage authorization of IT facilities and services of users who are violating these user rules (cf. §8);

i) to develop damage and risk prevention systems, based on automated data analysis, not including systems using personalised methods (such as SPAM-categorising and anti-virus scans of emails).

2. The IT departments have the obligation:

a) to support the users using the services and facilities (cf. §6) of the IT departments in consideration of the available capacities and to the best knowledge and believe. The users' responsibility for the technical content as well as the factual and computational accuracy of the achieved results remains unaffected;

b) to operate the IT-systems in consideration of economical, technical and organizational aspects for the user in the best possible way;

c) to take organizational measures to avoid loss of data, as well as unauthorised access, use or processing of data, in particular, unauthorised access to personal data;

d) to take reasonable steps to prevent further violations of current laws or the user rules in case of violations as mentions become known;

e) to inform the affected users in time in case of interventions in the availability of IT-systems, as well as in case of use of personal data and programs;

f) to record basic processes and consequences of data-analysing methods (cf. §7 article 1i ) and to inform affected users.

## §8
## Disciplinary measures

In case of violation of these user rules, current law, or further rules of the "Trier University of Applied Sciences" – as far as they affect the IT departments – disciplinary measurements can be executed, irrespective of any further considerations:

1. Issue a warning.
2. Temporary blocking of the user-ID.
3. Ban on entering the facilities of the IT departments (exclusion order).
4. Issue the causer an invoice for costs incurred as a result of misuse.
5. Eventually reporting to the contracting authorities of the user.
6. Make a complaint.

A user affected by exclusions 1-4 as listed above, may object to the exclusion in written form at the manager of the responsible IT department. The president decides about the objection after consulting the affected user as well as the manager of the responsible IT department.

## §9
## Liability

1. The user is liable for all damage caused deliberately while utilizing services of the IT departments.
2. All liability of the "Trier University of Applied Sciences" and the IT departments for damage of all kinds, that occur to the user while or because of utilizing the facilities and services of the IT departments, is excluded. The user is obliged to exempt the "Trier University of Applied Sciences" of any claims for damage.
3. The IT departments cannot guarantee the accuracy of results, achieved by using any services and IT-systems provided by the IT departments.

## §
## 10 Coming into force

These updated user rules, adopted by the senate committee of learning and teaching media, communication, and information supply of the "Trier University of Applied Sciences" become effective on November 18th of 2015.

**Trier, November 19th 2015**

**The management of the "Trier University of Applied Sciences"**