Trier University
of Applied Sciences

HOCHSCHULE TRIER

IT Policy of Trier University

Version 1.0
February 15, 2021

Content

1. Introduction

This IT guideline is intended to provide basic information on the use and handling of IT devices and applications within the IT infrastructure of Trier University. Furthermore, it is intended to provide rules of conduct with regard to data protection, IT and information security in addition to the technical measures taken by those responsible for IT.

2. Scope

This IT policy applies to all employees of Trier University of Applied Sciences. This includes all professors and employees (including part-time employees, trainees and student assistants and temporary staff). External persons who regularly use the IT infrastructure of Trier University are also required to comply with this policy.

3. Compliance with legal regulations

When using the IT systems and applications of Trier University, the applicable legal provisions on data protection and data security, copyright and the university regulations (in particular the user rules of the IT-departments[1]) must be observed. If there is any uncertainty in this regard, the supervisor should be consulted for clarification.

4. Training

The university shall ensure that employees receive the necessary training and instructions required for the respective handling of the IT systems and/or applications. Regular participation in training on information security and data protection at intervals of no more than three years is mandatory. New employees receive an information sheet with relevant instructions when they sign their contract. It is the responsibility of supervisors to ensure that employees from their area of responsibility regularly complete the training courses.

5. General regulations

Trier University of Applied Sciences provides its employees with IT systems and applications for the performance of their official duties. The installation of software on official devices for private purposes is prohibited. In addition, the general security guidelines and the corresponding license guidelines must be observed when installing software on official computers.

The use of private hardware or software for official purposes is at the user's own responsibility. Here, too, the general security guidelines and the corresponding license guidelines must be observed.

6. Workplace

The workplace must be designed in such a way that third parties without authorization have no access. Offices must always be locked after the last person has left their workstation. When leaving the workstation PC, the respective user must lock the workstation

so that authentication (user ID / password) is required before the IT system and/or application(s) can be used again.

In areas open to the public, the IT systems - especially the screens - must be set up in such a way that the risk of unintentional viewing by third parties is excluded as far as possible.

Information in paper form must be filed in such a way that third parties cannot gain knowledge of the data. Confidential information must always be kept under lock and key.

If the employee cannot carry out the measures to be taken on his own (e.g. due to constructional restrictions), this must be arranged via the supervisor.

7. Password use

As far as technically possible, all IT systems and applications must be set up in such a way that they can only be used after the user has been sufficiently authenticated. Authentication is usually performed by using the combination of user ID/password. Unless there are operational or technical reasons to the contrary, the IT-departments will assign a user ID and password to each individual authorized user.

Passwords must have a minimum length of 8 characters. The password must be alphanumeric (letters / numbers / permitted special characters). Each employee is obliged to change his / her initial password immediately.

Passwords must be chosen in such a way that they cannot be easily guessed. User IDs, first and last names, birthdays and names of relatives are not suitable for password selection. The same applies to trivially arranged number combinations (e.g. 12345).

Passwords that have already been used may not be reused when renewing a password. Under no circumstances should the password for the university ID be used for other (especially private) services. This also applies to administrative access via web or console to office multifunctional devices, printers, beamers, etc.

For managing multiple passwords, the proper use of an electronic encrypted password safe (for example, keepass or keeweb) is strongly recommended.

8. Protection against viruses and phishing attacks

Virus protection programs are used at the university to protect against malicious content (viruses, phishing). Both incoming and outgoing e-mail communication is checked by the virus protection programs used. Details on virus protection and the handling of virus-infected e-mails can be found in the amendements to the user ules of the IT-departments[2].

In the event that an e-mail is delivered with an unknown or suspicious file attachment or suspicious links, the attachment should not be opened or links activated under any circumstances. If the sender of the e-mail cannot be classified as trustworthy beyond doubt - e.g., by means of a valid digital signature - it is advisable to contact the respective IT-department.

To minimize the risk of viruses entering via other communication channels (malicious websites, USB sticks or other data carriers), every IT workstation must be equipped with an up-to-date virus scanner. Licenses are available from the data centers.

9. Protection against unsolicited advertising ("spam")

To protect against unsolicited advertising by e-mail, so-called spam filters are used in the IT-departments. Details on protection against SPAM mails can be found in the amendements to the user rules of the IT-departments[2].

10. Use of e-mail

Only the e-mail account provided by the university is to be used for work-related matters. Forwarding or linking to a private e-mail account is not permitted.

When transmitting personal data by e-mail[3], care must be taken to avoid disclosure of data, especially if this poses a high risk to the rights and freedoms of the data subjects.

Alternatives for data transfer are the cloud services provided by the university (see following section).

11. Use of cloud services

For work-related purposes, the university provides personal access to university cloud services (Alfresco, Seafile). The use of commercial cloud services (e.g. Dropbox, Google Drive, Microsoft OneDrive) is not permitted for the storage of personal or other sensitive official data.

12. Appointment coordination via internet

For the joint coordination of business appointments via the Internet, care must be taken to ensure freedom from advertising and conformity with data protection regulations. It is recommended to use the DFN Appointment Planner (Terminplaner.dfn.de).

13. Social media policy

The university has presences on various social media platforms that are maintained centrally by the Public Relations team. The Public Relations team must be notified of any additional, independent appearances in the name of the university. Responsibility for content lies with the person who initiated the establishment of this presence. This person is also responsible for compliance with applicable legal standards and must be evident within the appearance. With regard to the establishment and maintenance of a

social media presence, the guidelines of the „Bundesverband Hochschulkommunikation[4]“ must be observed.

14. Behavior in the event of security incidents

If it is determined that the protection or security of data may be compromised in any way (by virus attack, password compromise, or if there are other indications), a report must be made immediately to the supervisor as well as to the central e-mail address sicherheitsvorfall@hochschule-trier.de. This applies in particular if the threat relates to personal data.

Please direct general questions on the subject of IT security to informationssicherheit@hochschule-trier.de,

Please direct any questions regarding data protection to datenschutz@hochschule-trier.de.

Links to the attachments:

[1] User rules of the IT-departments
[2] Amendments of the IT-departments to the user rules
[3] Schutz personenbezogener Daten bei der Übermittlung per E-Mail
[4] Leitfaden des Bundesverband Hochschulkommunikation