TU/e Regulations for Computer and Network Usage

TU/e
EINDHOVEN UNIVERSITY OF TECHNOLOGY

DATE
01-11-2024

TU/e Regulations for Computer and Network Usage

Summary

Students and employees use a computer and internet almost every day for their studies and work. The TU/e would like to facilitate this by providing good ICT facilities and services. However, this also involves risks of improper use. Therefore, rules of conduct are needed for the use of TU/e ICT facilities and services.

The TU/e has laid down these rules of conduct in 'TU/e regulations for computer and network usage'. This describes how you as a user (student or employee of the TU/e or third party) may use the available ICT facilities and services, how liability is regulated and what measures the TU/e will take in case of misuse of the ICT facilities and services.

Basic rules

The aforementioned regulations set out in detail the conditions and procedures surrounding the use of ICT facilities and services. However, common sense and adherence to a few "ground rules" will get you a long way. We list the most important ground rules:

1. You may use the TU/e ICT facilities and services provided for private purposes (to a limited extent). It goes without saying that you will ensure that this does not interfere with your normal work (and that of others), and that you also apply the standards of decency and legality that normally apply when using TU/e ICT facilities and services.
2. Make sure that your activities do not overload ICT facilities and services. For example, do not send large volumes of messages or messages of such magnitude that they may slow down the system.
3. Use your username, password and e-mail address only personally; do not give this information to anyone else. Also be careful not to leave a computer you are logged into unattended. In case of misuse of your account, you are liable yourself.
4. Please ensure that messages you send are not hurtful, offensive, discriminatory, or otherwise inappropriate or unlawful.
5. It goes without saying that you will not use the ICT facilities and services for illegal activities, such as hacking, cracking security codes, committing fraud and illegally downloading or copying files.
6. Naturally, you do not send chain letters, advertisements or other "spam" messages.
7. Leave the system setting of TU/e facilities intact and handle the facilities provided with care.
8. You may not use the hardware and software provided by the TU/e for advertising or commercial purposes and you may not make them available to third parties. If you do so and TU/e is fined, this fine will be passed on to you.
9. If you use private devices for work- or study-related activities, you are bound by TU/e's Mobile Device and Teleworking Policy. You can find these on the intranet.

Procedures and measures

If improper use as referred to above of TU/e's computer and network facilities is suspected, TU/e may take steps against it. For example, under certain circumstances the TU/e is obliged to make data and/or files from a computer available if authorities with a legal basis request this. The TU/e can also initiate an investigation if it suspects misuse. Of course, in doing so, the TU/e adheres to the rules as described in the General Data Protection Regulation.

Should there indeed be unlawful use of the TU/e ICT facilities or services, the TU/e is obliged to take follow-up action. Reports of misuse will proceed as described in these regulations. Sanctions vary depending on the

severity of the violation.

Learn more

Below you will find the complete computer and networking regulations.

TU/e Regulations for Computer and Network Usage

The Executive Board of Eindhoven University of Technology (TU/e), having regard to Article 7.57h and 9.2 of the Higher Education and Scientific Research Act (WHW) insofar as students and third parties are concerned, and with regard to employees who are employed, having regard to (also) the labor law rights and obligations that apply, arising from, inter alia, the Dutch Civil Code, the General Data Protection Regulation, the Collective Labor Agreement (CAO) of Dutch Universities, any other collective regulations and the individual employment contract.

DECIDE to withdraw:

- TU/e Regulations for Computer and Network Usage 2022

ADOPT:

- TU/e Regulations for Computer and Network Usage 2024, reading as follows:

Chapter 1 - General

Article 1 Definitions

For the purposes of these regulations, the following definitions shall apply:

Director:	The director of operations of a faculty, or the director of a department.
Competent authority:	The TU/e Executive Board is the competent authority. The Executive Board may mandate the Department Board, the Director or the Chief Information Security Officer to act as the competent authority.
CERT:	Computer Emergency Response Team.
CCNG:	Computer and Network Use Committee.
Third Party:	A User who is not an employee or student and is a guest of TU/e.
User:	Anyone who, with the consent of the Competent Authority, makes use of the ICT facilities and services made available by TU/e. This consent is evidenced by username, email address and/or other access code provided by the Competent Authority or by acceptance of the Terms of Use in the case of the guest network (wi-fi). These Users in any case include Students, Employees, staff hired by TU/e, externals and guests.
ICT facilities:	The computer and network facilities provided by or on behalf of TU/e, including electronic equipment, such as (desktop) computers, laptops, notebooks, tablets, cell phones and printers, and software, (licenses) such as software, computer operating systems and other computer and/or network facilities, such as the physical and wi-fi network (the secure network and guest network).
ICT services:	The facilities provided by or on behalf of the TU/e for electronic information exchange, including but not limited to (access to) the Internet, intranet, e-mail, library information systems, social media accounts and/or chat groups and all other electronic facilities that are accessible with or without an access code or via a link, as

	well as connection facilities for the purpose of electronic equipment.
Report:	Notification submitted in writing (including electronically) concerning improper or unauthorized use of the ICT facilities and services by a User.
Misuse:	Use of the ICT facilities and services in violation of the Regulations and/or a relevant (unwritten) rule of law whether in minor or major form as referred to in Appendix 1 to the Regulations.
Social media:	For example, but not limited to Facebook, YouTube, Instagram, Skype, WhatsApp, Twitter or LinkedIn.
Student:	Anyone who is enrolled at TU/e as a student or is taking education at TU/e (full-time or part-time or on the basis of a special form of enrollment).
Regulations:	The present Regulations for Computer and Network Usage.
Employee:	The employee as referred to in the Collective Agreement for Dutch Universities who is employed by the TU/e, or temporarily employed through EuFlex, or personnel hired by the TU/e, such as guest lecturers and external staff for the purpose of projects.

Chapter 2 - Principles

Article 2 Objective

2.1 The Regulations establish rules regarding the use by Users of the ICT facilities and services provided by TU/e. These rules aim in particular to:
- secure ICT facilities and services, including security against damage and misuse;
- protect confidential information and intellectual property of TU/e;
- protect (personal) data of Users;
- manage cost and capacity.

Article 3 Scope

3.1 The Regulations apply to all use of ICT facilities and services provided by TU/e, regardless of where and how they are used or logged in.

3.2 The Regulations apply to all Users, whether or not they are present at the TU/e.

Article 4 (Private) use

4.1 The ICT facilities and services used by the User serve primarily and predominantly for the education of and research for the program for which the User is enrolled, or for the performance of the User's job, or for the purpose for which the User is present at TU/e.

4.2 In addition, the User is permitted to use the ICT facilities and services for private purposes to a limited extent, provided that this does not interfere with their normal work activities and does not offend others. Nor may the aforementioned private use in any case place an unreasonable burden on TU/e's ICT facilities and services or conflict with licenses held by TU/e or with intellectual property or other rights of TU/e and/or others.

4.3 The storage of private files or information on TU/e ICT facilities and services is permitted, provided that Art. 4.2 is complied with. Private files must be kept in a (sub)folder named 'Private' or 'Personal' clearly separated from other work- or study-related data. TU/e is not obliged to make back-up copies of these files or to make copies available in the event of

replacement or repair of the systems concerned.

4.4 After the death of an employee or student who uses a TU/e device (such as a laptop or cell phone), the TU/e can, at the request of next of kin, share files or make copies available to next of kin that are stored in a folder or sub-folder called 'Private' or 'Personal'. Only personal files stored in this way on a TU/e device can be shared with next of kin. Files not saved in this manner, or work files, will not be shared with next of kin.

4.4 The email address and associated mailbox provided by TU/e are made available exclusively for use in the context of teaching and research for the program for which User is enrolled, or for the purpose of performing User's job.

4.5 The User is obliged to use TU/e's email facilities for use within the framework of teaching and research for the program for which the User is enrolled, or for the purpose of performing the User's job.

Article 5 Use of private equipment by Employees

5.1 TU/e shall in principle provide the equipment necessary for the performance of the work in the context of the Employee's position. The Employee is therefore not permitted to use their own equipment for the performance of this work.

5.2 The use of an Employee's own cell phone (such as calling and sending and receiving text messages, e-mail and sending and receiving files and/or logging in by means of an authentication app) in the performance of the work is permitted as part of the Employee's job, provided adequate security measures are in place. At a minimum, the Employee is expected to have the following security measures in place:

- secure the cell phone with a password or PIN. If possible, the cell phone can also be secured by facial recognition or fingerprint;
- lock the cell phone when left unattended;
- do not store any personal data for which TU/e is responsible (other than contact information) on the cell phone;
- separate (encrypted) TU/e data from private data. This separation must be clearly recognizable on the cell phone (see also Art. 4.3);
- keep software up-to-date by performing periodic updates;
- take adequate measures against viruses or malware by installing antivirus software, keeping it up-to-date and scanning the cell phone regularly (at least monthly).

Article 6 Dealing with confidential information

6.1 User must keep confidential information, including personal data, strictly confidential and take adequate measures to ensure confidentiality. Confidential information includes any data or information expressly marked or identified as confidential by the providing party. In addition, it includes any information that, because of its nature or the circumstances of its disclosure, would reasonably be considered confidential.

6.2 In the event of theft or loss of equipment on which TU/e data are present, the User must report this immediately.[1] The User must cooperate in the removal of TU/e data present on the equipment, insofar as this is technically possible. For equipment owned by TU/e, such removal action can take place without the intervention of the User.

[1] Link data breach form https://www.tue.nl/en/our-university/about-the-university/support-services/library-and-information-services/privacy-security

Chapter 3 - Use of ICT facilities and services.

Article 7 Prescribed systems

7.1 TU/e may prescribe systems or applications for educational, research and other business purposes, such as an electronic learning environment, an email system or multimedia services. User is obliged within the framework of education of and research for the program for which User is enrolled, or for the purpose of performing User's job, to use the prescribed systems or applications and to strictly comply with restrictions. These prescribed systems or applications serve primarily and predominantly for the education of and research for the program for which User is enrolled, or for the purpose of performing User's job duties, and private use is permitted only if Article 4 and Article 5.2 of these regulations are complied with.

Article 8Following directions or instructions

8.1 User shall comply with general instructions given by or on behalf of TU/e for the use of ICT facilities and services.

8.2 When using the ICT facilities and services, the User is obliged to identify themselves by means of the username and/or email address provided to them by the Competent Authority, if applicable by means of password. The User is obliged to keep their username and password strictly confidential and not to disclose the username nor the password to any other person.

8.3 At the request of the Competent Authority, each User shall promptly demonstrate residency at TU/e by means of their campus card at the time the User uses physical facilities.

8.4 User shall not misuse the ICT facilities and services provided by the Competent Authority as well as username, password and email address.

Article 9 Use of social media

9.1 Social media are permitted with due observance of these Regulations for matters concerning the User's function or performance. However, the User must be careful not to harm the good name of TU/e and the User. In other words, Social Media must be used responsibly.

9.2 The TU/e supports an open dialogue, the exchange of ideas and the sharing of the User's knowledge with others through Social Media. For related topics, the User must ensure that the profile and content match how the User would present themselves to others in text, image and sound.

9.3 Directors, managers, team leaders and others who promote policy or strategy on behalf of TU/e have a particular responsibility when using Social Media, even if the content is not directly related to their work. Based on their position, they should consider whether, if applicable, they can publish in a personal capacity. They should be aware that others read what they write.

9.4 Sharing or disseminating other people's personal data via Social Media in a professional capacity is only permitted if it is part of the employee's regular work and has been reviewed for compliance with the GDPR and other applicable laws. Extra attention should be paid to the dissemination of visual material (photos and videos) in which others can be identified; this usually requires the explicit consent of the individuals concerned.

9.5 This article also applies when TU/e ICT facilities and ICT services are not used.

Article 10 Prohibited uses

10.1 With respect to the use of the ICT facilities and services, the User is in any case not permitted to:

a. Cause material or immaterial damage to TU/e or others;
b. Infringe on the rights of TU/e or others;
c. Cause a nuisance or disturb public order;
d. Act in violation of applicable law, including those arising from intellectual property laws, including the Copyright Act, the Benelux Trademark Act, the Neighboring Rights Act, the Databases Act as well as rights arising from the Penal Code, the General Data Protection Regulation or with rights arising from the Civil Code, more specifically article 6:162 et seq;
e. Act contrary to what is proper in society according to unwritten law;
f. Use another person's username, password and/or mail address or other personal access data of others. If this does occur, such use by the other will be attributed to the rightful holder of the username, password and/or mail address or other access data;
g. Use a different or feigned username, password and/or mail address, or otherwise attempt to conceal their identity;
h. Obtain unauthorized access to another's data, files and/or computer systems (including wardriving, sending cookies, junk mail, etc.), whether by hacking or otherwise, including breaking or cracking a security code;
i. Break or crack a security or security code;
j. Send, post, make accessible by hyperlinks or otherwise make public any messages or communications, the content of which is offensive, lewd, discriminatory, inflammatory, defamatory, offensive, abusive, hurtful, indecent or otherwise contrary to public order or morality or may otherwise be deemed unlawful;
k. Send, post, make accessible by hyperlinks or otherwise make public large quantities of messages or messages of large size, which the user knows or could or should have known may cause interference, inconvenience and/or delay within the system, or to the recipient(s);
l. Send unsolicited messages, post them, make them accessible by means of hyperlinks or otherwise make them public, of which the User knows, or could or should have known, that the posting is not for the benefit of recipient(s) nor was done in the context of training or performance of duties.
m. Intentionally send, post, make accessible through hyperlinks or otherwise disclose messages or communications that the User knows, could or should have known to be false.
n. Send, post, make accessible by hyperlinks or otherwise disclose chain letters, advertising messages and similar messages.
o. Make ICT facilities and services available to others.
p. Keep the ICT facilities and services unnecessarily occupied. This includes not only keeping a facility or provision in use without the user being physically present, but also using the ICT facilities and services for a purpose other than the purpose described in clause 4.1.
q. Leave, abandon or leave open the ICT facilities and services in such a way that others are given the opportunity to use or Misuse the Facility and/or Service.
r. Use the ICT facilities and services unlawfully or for illegal or abusive purposes.
s. Make changes to (system) settings of TU/e ICT facilities and services.
t. Infect the ICT facilities and services with a virus.
u. Use the ICT facilities and services for advertising and for commercial purposes. In the event that this provision is violated and a fine is imposed on TU/e, this fine will be passed on to the person who did not comply with this provision.
v. Use the ICT facilities and services to commit fraud, for example, in testing.
w. Use the ICT facilities and services to bind TU/e in any way in violation of mandates or powers of representation, including agreeing to license terms that are binding on the entire university.

10.2 Use of the ICT facilities and services in violation of Article 4.1, 4.2 and/or use that falls under Article 10.1 shall be considered Misuse.

10.3 Prohibited and risky use of the ICT facilities and services will be made impossible as much as possible by technical means, for example by block-listing high-risk applications.

Article 11 Management measures

11.1 Library & Information Services is authorized, in the interest of the ICT facilities and services or parts thereof, or in the interest of the traffic over the ICT facilities and services, to take actual measures that may be detrimental to the User and/or the use of the ICT Facilities and services without this giving rise to TU/e liability.

11.2 The Director of Library & Information Services shall have discretionary authority with respect to communications regarding the provisions of Article 11.1 and/or explanations of actions taken.

Article 12 Access to email and files

12.1 Statutory regulations and/or rulings by a judicial authority may oblige the disclosure of data (files) of User(s) stored or accessible via the ICT facilities and services. In such cases the competent authority is authorized to allow access to these data (files), or to download or copy them for the purpose of complying with the relevant obligation. Users shall cooperate with this.

12.2 In the event of an Employee's death, illness/incapacity or unexpected prolonged absence, it shall be permissible by order of the Authority to provide a substitute or supervisor with access to the Employee's files or mailbox if:
- this constitutes a compelling reason of business interest, and
- obtaining consent from the Employee is impossible, and
- prior separate approval is obtained from a supervisor of the Employee. [2]

12.3 The aforementioned substitute or supervisor may not, however, access folders marked as private, emails identified as private, or emails sent to or originating from a person in a position of trust assigned by the Executive Board. If the Employee has not made such markings, the Authorized Executive may, through the use of a confidential officer, review the Employee's relevant information in order to recognize and set aside private information before the replacement or supervisor is granted access.

12.4 If it is suspected that TU/e data are nevertheless present in folders and/or e-mails of the Employee classified as private, the procedure as stated in Art. 14 applies.

Chapter 4 - Monitoring, control and targeted research

Article 13 Monitoring of use of ICT facilities and services

13.1 Monitoring and control of the use of the ICT facilities and services shall take place (preventively) in the context of enforcement of the rules of these Regulations for the purposes in Art. 2.

13.2 For the purpose of monitoring security and integrity and ensuring the proper functioning of

[2] Topdesk - KI2687

the ICT facilities and services provided, traffic and usage information is processed (logged) automatically and analyzed on a regular basis. These automated procedures result in the signaling of a particular security risk. In response to this signaling, preventive and corrective measures can be taken (automatically or not).

13.3 Some measures that TU/e can exercise for control are:
- Monitoring based on automated scanning of content, such as email filtering, virus scanners and monitoring of network traffic to prevent rogue files and spam. Without concrete cause, the confidentiality of communications remains guaranteed;
- Monitoring in the context of cost and capacity control will be limited to automated tracking of sources of cost or capacity demand (such as the addresses of Internet radio and video sites) based on traffic data. If these sites result in high costs or nuisance, they will be blocked or throttled, striving not to violate the confidentiality of the content of communications;
- Monitoring to improve the security of ICT facilities and assets and to prevent cybersecurity incidents. This surveillance can be done, for example, using attack simulations, such as security penetration testing and social engineering, such as phishing campaigns.

13.4 TU/e shall fully comply with the General Data Protection Regulation and other relevant laws and regulations when monitoring at the level of traffic and usage information. In particular, TU/e secures the data recorded during monitoring against unauthorized access and persons with access to it are contractually obliged to maintain confidentiality.

Article 14 Targeted investigation following suspicious indications

14.1 Targeted investigation occurs when traffic data or other personal data concerning one or more specific Users are recorded in the context of suspicious indications. The purpose of this investigation is to find out whether there is actually a violation and to what extent and with what measures any risks can possibly be mitigated.

14.2 Directed examination will take place only after a proportionality and subsidiarity test by CERT, CCNG or the Examination Committee, in the following cases only:
- Serious suspicion of violation of these Regulations
- Serious suspicion of, inter alia, breach of the (network) security, integrity and continuity of ICT facilities and services
- Order/request to do so from an (inter)national authority (e.g. police or judiciary)
- Serious suspicion of violation of laws and regulations, e.g. criminal violations and/or procedures regarding knowledge security.

Targeted investigation in response to automatic signals (monitoring)

14.3 CERT is authorized to conduct targeted research in response to automated procedures resulting in the identification of a particular security risk, as described in Article 13. This investigation will initially be limited to the level of individual metadata (traffic data) of e-mail and Internet use, and only in the event of compelling reason(s) will an investigation into the content take place.

Other targeted research (e.g., in response to requests and/or Reports)

14.4 Directed research other than in response to automated procedures resulting in the signaling of a particular security risk, as described in Article 13, for example in response to a request and/or Report, will only take place after a proportionality and subsidiarity test, and after advice from the CCNG or a request from an Examination Committee, the latter if it concerns matters of assessment and examination of Students.

14.5 Inspection of privacy-sensitive information or personal data of individuals will be limited as much as possible. Targeted investigation will initially be limited to the level of individual metadata (traffic data) of e-mail and Internet use. Where possible, only automated monitoring or filtering will be performed, without gaining insight into the behavior of individuals. There will always be a balancing of interests between safeguarding the security and integrity of the ICT facilities and services and protecting the privacy of the User. Only in the event of compelling reasons will a targeted investigation of the content take place.

14.6 The data collected during a targeted investigation are only accessible to system administrators of the department concerned, other Employees or external parties for whom access is necessary and who have been engaged to further analyze the report. Investigation results are further shared with the Competent Authority and/or an Examination Committee, the latter if it involves matters of assessment and examination of Students. To other administrators or employees involved in the execution of the investigation, these data are made available anonymously if necessary in principle, and pseudonymized if this is not possible.

14.7 If the CCNG or an Examination Committee has requested a focused examination, and it later turns out that it was not the competent body, it will transfer this to the competent body (CCNG or Examination Committee).

14.8 In urgent cases, when this is necessary to safeguard the continuity and quality of the primary business processes of TU/e, a targeted examination may take place without the advice of the CCNG or an Examination Committee. The case must then be submitted for review to the CCNG or an Examination Committee as soon as possible after the targeted research has taken place.

14.9 The User will be informed in writing as soon as possible by the Competent Authority of the reason, execution and result of the investigation. The User will be given the opportunity to explain the data found. The obligation to provide information to the User can only be postponed if this could harm the investigation.

Article 15 Notifications and procedure to be followed

15.1 Reports about one or more Users can only be made in writing via e-mail address ccng@tue.nl. Reports made elsewhere within TU/e will be forwarded to the CCNG's e-mail address.

15.2 If the CCNG receives a Report regarding assessment and examination of Students, it will forward it to the Examination Committee, which will then handle this Report independently.

15.3 Each Notification must be substantiated, clearly described, and at a minimum must include:
- Time period during which the alleged Misuse occurred;
- What the suspected Misuse consists of;
- By which User(s) the suspected Misuse occurred;
- What data is necessary to establish suspected Misuse.

15.4 The CCNG may enter into discussions with a Reporter in order to obtain more information and will do so in any case when a Report is not complete (in accordance with Art. 15.3). If the Reporter is unable to complete the Report, the CCNG will ask the Competent Authority to supplement the Report. In all other cases, the CCNG will always inform the Competent Authority of the Report received.

15.5 The CCNG will decide whether the Report is (manifestly) unfounded, in which case it will not consider the Report. If the CCNG does take up the Report, it will give advice on whether or not

to conduct a targeted investigation as described in Art. 14.

Article 16 The Computer and Network Use Committee (CCNG).

16.1 The CCNG receives Reports about Users and advises the Competent Authority regarding the conduct of any targeted investigation as defined in Article 14.

16.2 The CCNG consists of:
1. ICT expert (chair)
2. Privacy expert
3. Director of a department (representative of the Competent Authority).
4. Legal expert
5. Ethical expert

The committee is assisted by a secretary from the LIS Department.
Members of the CCNG are appointed by the Executive Board for a four-year term.

16.3 If the Report states that only metadata (traffic data) is required to establish the suspected Misuse, the CCNG will decide with paragraphs 1 through 3 on whether or not to conduct a targeted investigation as described in Art.14. If the Report states that (also) investigation on content is necessary, then the CCNG decides with the full number of members.

16.4 The CCNG is authorized, if it deems it necessary for the performance of its work, to do whatever is necessary to carry out its duties.

16.5 The CCNG has regulated its operating procedures in by-laws.

16.6 The CCNG shall prepare an annual report of its activities, which shall be made publicly available.

Chapter 5 - Measures

Article 17 Blocking of ICT facilities and services

17.1 In the event of acting contrary to these Regulations, violation of laws and regulations or a serious breach of (network) security, integrity and continuity, the Competent Authority may take appropriate measures, with or without the assistance of system administrators, depending on the nature and seriousness of the breach. In addition, the Competent Authority may decide to restrict, temporarily or otherwise, access to certain ICT facilities.

17.2 These will always be temporary measures that will not be maintained any longer than necessary. If the situation permits, the competent authority will assess in advance whether the measure is appropriate, weighing up the interests involved between safeguarding the security and integrity of the ICT facilities and services and protecting the user's privacy. In urgent cases, the CERT has the mandate to take measures without an order from the Competent Authority, on the understanding that the case will still be submitted to the Competent Authority for review as soon as possible after the targeted investigation has taken place.

17.3 Measures (other than a warning or temporary blocking) cannot be taken solely on the basis of automated processing of personal data. In the case of a warning based on automated processing, the employee shall be given an opportunity to express their views.

Article 18 Sanctions against Students

18.1 If an Examination Committee has dealt with a Report or has requested a focused investigation

as described in Art. 14, the Examination Committee may impose a sanction in accordance with the Examination Committee regulations.

18.2 The Competent Authority may take one or more of the following measures and/or sanctions against the Student who has violated the provisions of these Regulations as well as against the person whose username, password and/or e-mail address was used for said violations:

a. A written warning including a written warning with conditions.
b. The prompt removal or blocking of information. This may include removing or blocking other information from Student. The Student is liable for all damages resulting from the removal or blocking of information as referred to in this article, including when doing so removes or blocks information other than Student's information;
c. Conditional or unconditional denial of access to and/or use of the ICT facilities and services and/or use of the username, password and/or e- mail address and/or conditional or unconditional denial of access to (a part of) the TU/e buildings and/or grounds;
d. Reporting a criminal offense.

18.3 In giving or determining the sanction, the Competent Authority may use Appendix 1: examples of classification of different forms of misuse regarding computer facilities.

Article 19 Sanctions against Employees

19.1 For TU/e Employees, failure to comply with these regulations will result in a labor law measure by the Competent Authority, for example, a warning, transfer, suspension or termination of the employment contract.

19.2 Labor law measures cannot be taken solely on the basis of automated processing of personal data and will only become final after the Employee has been given the opportunity to express their views.

19.3 In giving or determining the sanction, the Competent Authority may use Appendix 1: examples of classification of different forms of misuse regarding computer facilities.

Chapter 6 - Final and transitional provisions

Article 20 Scientific research

20.1 For scientific research, an exception to Art. 10 (Prohibited Use) may be made by the Director of LIS, provided that the research has been approved by TU/e's Ethical Review Board.

20.2 Traffic and usage information obtained by monitoring the use of ICT facilities and services (as described in Art. 13 Monitoring the Use of ICT Facilities and services) may be used for scientific research, provided that the research has been approved by TU/e's Ethical Review Board and approval has been given by the Director of LIS. These data are preferably made available anonymously or pseudonymized.

20.3 The above-described data used within scientific research may only be shared with other (scientific) partners/parties if this has been approved by the Director of LIS and TU/e's Ethical Review Board. This is preferably done anonymously or pseudonymously.

Article 21 Liability

21.1 The TU/e excludes all liability for damage arising from the use of and inability to use or fully use the ICT facilities and services. This applies unless TU/e can be blamed for intent or gross

negligence.

21.2 The User is liable for any damage caused by acting contrary to these Regulations or contrary to the care that may be expected of the User. This also includes the damages that a third party claims from TU/e as a result of these actions.

Article 22 General Administrative Law Act

The procedures set forth in these Regulations are open to students only for objections and appeals under the General Administrative Law Act, to the extent that

a. there is a decision within the definition of the General Administrative Law Act.

Article 23 Applicable law

If disputes arise under these regulations or under other regulations or agreements, Dutch law shall apply. The competent Dutch court, to the exclusion of other courts, shall have jurisdiction to hear disputes.

Article 24 Annexes

One Appendix accompanies the Regulations. The Appendix may be amended by the Authorizing Authority. The amended Appendix will be published on the TU/e website before it takes effect.

Article 25 Implementation

25.1 These regulations may be cited as Regulations for Computer and Network Usage.

25.2 These regulations shall enter into force on November 1, 2024, and replace the regulations as adopted on January 1, 2023

Adopted by the Executive Board at its meeting of September 26, 2024, after approval by the University Council.

Appendix 1: Examples classification of different misuses related to computer facilities

This classification is an example of application of the Arrangement. The examples are indicative, not exhaustive.

Minor forms of misuse

Nuisances including:

- Games
- Sound
- Chat
- Screensavers, background screens
- Redundantly occupying hardware and peripherals
- Excessive network load

Major forms of misuse

- Racist expressions
- Sexist expressions
- Swearing
- Pornography
- Illegal copying
- Hacking
- Data manipulation
- Distribution of viruses and illegal software
- Email bombs/junk mail
- Intentionally damaging hardware and peripherals
- Reading through e.g. a robot or script files provided by the library, when they should only be used according to the license terms