Technische Universität Dresden

Regulations for the Information Technology Equipment and Services and for Information Security at TU Dresden (IT Regulations)

Dated: February 18, 2021

On the basis of § 13 (5) (1) of the Higher Education Freedom Act of Saxony in the version of the announcement of January 15, 2013 (SächsGVBl. p. 3), last amended by Article 5 of the Act of December 17, 2020 (SächsGVBl. p. 731), at its meeting on February 18, 2021, the University Executive Board of Technische Universität Dresden issued the following regulations.

Contents

Section 1: General Provisions

§ 1
Scope

(1) These regulations apply to the operation and use of IT infrastructure at TU Dresden as well as to its users.

(2) The IT infrastructure of TU Dresden is understood to include all information technology facilities, IT systems (hardware and software), and IT communication networks as well as the services provided (including VoIP).

(3) These regulations may be specified in more detail by more extensive implementation regulations, provided that this does not violate the provisions of these regulations.

(4) The provisions of these regulations must be observed in agreements and contracts with institutes affiliated with TU Dresden as well as non-university institutions that are directly affiliated with the network of TU Dresden or are participants in the German National Research and Education Network (DFN) via this network.

(5) The freedom of science, research, and teaching remains unaffected by these regulations, particularly if their subject is IT research.

§ 2
Object of the Regulations

The object of these regulations are the options and rights of use with regard to the IT infrastructure of TU Dresden and related conditions as well as the obligations resulting from its use. Furthermore, the responsibility structures required for a university-wide information security process, the assignment of tasks, and the cooperation of the parties involved are defined.

§ 3
Definitions of Terms and Regulatory Content

(1) Users in the sense of these regulations are all natural persons and legal entities of the closed user group who make use of the IT infrastructure of TU Dresden with its associated services for purposes pursuant to § 14 (1) and (3).

(2) The closed user group consists exclusively of members and affiliates of TU Dresden as well as other natural persons (guests) who fulfill the requirements pursuant to § 14 (2) (2).

(3) A third party is any natural and legal person outside the closed user group.

(4) Administrators in the sense of these regulations are persons responsible for the content and technical aspects of TU Dresden's IT infrastructure, as well as persons authorized to control it. Only members or affiliates of TU Dresden are allowed to act as administrators. Exceptions are defined in § 13.

(5) Processing is the collection, storage, modification, anonymization, transmission, use, provision, blocking, and deletion of data, irrespective of the procedures used.

(6) User account in the sense of these regulations are all data, in particular ZIH login, password, and email address, which are assigned to a user for the proper use of TU Dresden's IT infrastructure with its associated services.

(7) User ID in the sense of these regulations is the login and password for the Center for Information Services and High Performance Computing (ZIH).

(8) DFN-PKI in the sense of these regulations is the public key infrastructure of the German National Research and Education Network, in which the TU Dresden participates. An advanced electronic signature is provided. The certification guidelines of the DFN-PKI are binding here. The advanced signature from the DFN-PKI is to be used at TU Dresden, unless the requirement of written form is stipulated by a legal regulation or contracts or contractually agreed.

(9) IT processes are the totality of all facilities and services in which data are processed for a specific purpose to be specified.

(10) Information security is to be regarded as a comprehensive term for the protection of information and, irrespective of the method of processing, refers to the protection of all relevant information, including personal data. In this context, information security refers in particular to a state in which the risks to the security objectives of confidentiality, integrity, availability, authenticity, auditability, and transparency of information and IT are reduced to an acceptable level by appropriate technical and organizational measures.

(11) An IT emergency is a prolonged failure of IT processes or IT resources with high or very high levels of damage.

Section 2: Responsibilities, Authorities, and Liability

§ 4
TU Dresden

(1) TU Dresden shall ensure that IT infrastructure and services are available to users at TU Dresden for use for purposes pursuant to § 14 (1) and (3).

(2) TU Dresden does not assume any guarantee that the information technology facilities and services as well as the software used at TU Dresden are error-free and available at all times without interruption. Potential data loss as a result of technical disruptions and the disclosure of confidential data through unauthorized access by third parties cannot be ruled out.

(3) TU Dresden assumes no responsibility for the software provided. Furthermore, TU Dresden shall not be liable for the content, in particular for the correctness, completeness, and timeliness of the information to which it merely provides access for use.

(4) Moreover, TU Dresden shall only be liable in the event of gross negligence and intent on the part of its employees, with the exception of damages resulting from injury to life, limb, or health. The limitation of liability shall also not apply in the event of a culpable breach of essential obligations, compliance with which is of particular importance for the achievement of the purpose and TU Dresden is aware of this. In this case, the liability of TU Dresden is limited to damages that are typical and foreseeable at the time of the user relationship is established. No liability is assumed for indirect or consequential damages.

§ 5
CDIO

(1) The CDIO (Chief Officer for Digitalization and Information) shall develop strategies for digitalization in teaching, research, and administration as well as for the responsible use of IT. He/she is responsible for the further development of IT services as well as safeguarding IT equipment and IT administration at TU Dresden and monitors their implementation.

(2) The CDIO is a member of the Extended University Executive Board.

(3) The CDIO is supported by a strategically focused body, the CDIO Strategy Council. The CDIO Strategy Council consists of

1. the School CDIOs
2. the CDIOs of the Central Academic Units, Carl Gustav Carus University Hospital, and the Saxon State and University Library, insofar as they are not members in personal union pursuant to number 1
3. the Head of the Planning and Organisation Directorate and the Head of the Information Security Unit as representatives of Central University Administration
4. the Director of the Center for Information Services and High Performance Computing (ZIH).

The CDIO shall chair and convene the CDIO Strategy Council.

(4) Furthermore, the CDIO is supported by the IT coordinating team. It addresses issues and agreements relating to the operational management of the IT infrastructure and the underlying services and can submit proposals for resolutions in this regard to the CDIO Strategy Council. The IT coordinating team consists of the IT Advisors of the Schools and the Central Academic Units as well as representatives of all member groups of the university. The CDIO shall chair and convene the IT coordinating team.

(5) To prepare their decisions, the CDIO may, in particular, set up work and project groups consisting of members from specific topics or disciplines.

§ 6
Information Security Unit

(1) The responsibility for establishing and maintaining an appropriate level of state-of-the-art information security on an ongoing basis rests with the Extended University Executive Board, represented by the CDIO. The Extended University Executive Board shall establish the Information Security Unit to perform information security tasks. The unit acts independently in the performance of its duties in this regard. Article 38 of the EU General Data Protection Regulation (GDPR) of April 27, 2016 and § 8 (2) of the Information Security Act of Saxony (SächISichG) remain unaffected.

(2) The Information Security Unit includes at a minimum the Data Protection Officer of TU Dresden, the Information Security Officer of TU Dresden, and the TUD-CERT.

(3) The Information Security Unit is under the direction of the Data Protection Officer. The TUD-CERT is under the direction of the Information Security Officer.

(4) The Information Security Unit provides appropriate processes, action plans, and response plans in coordination with the CDIO and the Extended University Executive Board to ensure compliance with security objectives.

§ 7
Center for Information Services and High Performance Computing (ZIH)

(1) The Center for Information Services and High Performance Computing (ZIH) is generally responsible for the central IT infrastructure of TU Dresden. The services shall be documented in a business service catalog that is updated on an ongoing basis. The operation of further central services by other structural units is possible in agreement with the CDIO.

(2) Following technical development, ZIH shall take the necessary measures to prevent and eliminate the misuse of IT systems. The establishment and operation of central security-related facilities and services is generally the responsibility and purview of ZIH. In the case of significant measures, especially those affecting all of TU Dresden, the CDIO shall decide. Users shall be informed of the necessary measures in a timely, transparent, and clearly understandable manner.

(3) The installation and operation of active network components in decentralized purview and responsibility shall only be permitted in consultation with ZIH and in agreement with the CDIO. If VoIP facilities are operated in data distribution rooms, these rooms shall be assigned to ZIH and shall be used exclusively for the purpose of operating the data communications network. Access to these data distribution rooms shall be determined by ZIH at its due discretion and in particular pursuant to § 19 (1). If TU Dresden's infrastructure is not provided centrally, it may be operated under the responsibility of the Schools in agreement with ZIH and the Information Security Unit as well as in agreement with the CDIO.

(4) The details of the options for use and conditions of use of the facilities and services pursuant to § 7 (1) to (3) are defined by ZIH in its regulations for use.

(5) The provisions of § 7 (1) to (4) shall apply accordingly to other structural units of TU Dresden if they provide and operate central IT infrastructure.

§ 8
Decentralized IT Organization

(1) The School CDIOs and the CDIOs of the Central Academic Units are specifically responsible within their area of responsibility for:

1. the implementation of the digitalization strategy specified by the Extended University Executive Board and the decisions made by the CDIO
2. the strategic planning and development of IT-based services as part of each structural unit
3. the implementation of the provisions of these regulations for all information technology facilities operated in each structural unit with the associated services

(2) The School CDIOs and the CDIOs of the Central Academic Units are nominated by the head of the structural unit to which they belong and are appointed by the CDIO. For issues relating to digitalization and information security, the heads of the Schools shall involve the School CDIO. The CDIOs of the Central Academic Units must coordinate their activities accordingly with their management. The School CDIOs and CDIOs of the Central Academic Units shall be supported by the heads of the Schools and the Central Academic Units in implementing the digitalization strategy and ensuring IT-based services.

(3) To fulfill the assigned responsibilities, the School CDIOs and the CDIOs of the Central Academic Units are supported by an IT Advisor.

(4) Decentralized IT provision and administration is carried out by (decentralized) IT service teams.

(5) The IT Advisor is authorized to give instructions to the IT service teams (which consist of the IT administrators of the structural units), if any, for the implementation of the tasks of the School CDIOs and the CDIOs of the Central Academic Units specified in (1).

(6) Users in the sense of these regulations are required to observe the instructions and specifications of the School CDIOs and CDIOs of the Central Academic Units.

§ 9
Head of the Structural Unit

(1) The head of the structural unit is responsible for compliance with the provisions of these regulations in his/her area of responsibility.

(2) He/she must appoint one or more persons responsible for the IT infrastructure in his/her area of responsibility. Their appointment shall be reported to the IT Advisor assigned to them. Changes shall be reported on an ongoing basis.

(3) The head of the structural unit shall appoint a process owner for his/her own IT infrastructure, who shall document this IT infrastructure.

§ 10
Special Rights and Duties of Administrators

(1) The administration of the IT infrastructure pursuant to § 1 (1) must be cooperative, appropriate, and for the intended purpose. In particular, the provisions on data and telecommunications secrecy and the principles of data avoidance and minimization must be observed.

(2) Administrators are required to keep track of sources of information about security issues and respond to information about how to fix security vulnerabilities.

(3) The administrators are responsible for the technical organization and implementation of data protection and data security measures.

(4) In the case of decentralized user administration pursuant to § 15 (5), the administrator shall, in particular, manage the user authorizations and inventory data granted to users within his/her area of responsibility.

(5) The administrator is also entitled, with the help of automated methods, to document and evaluate the use of the data processing systems and software by individual users, but only to the extent that this is

1. to ensure proper system operation,
2. for resource planning and system administration,
3. to protect the personal data of other users,
4. for billing purposes,
5. for the timely detection and elimination of system vulnerabilities and disruptions or for troubleshooting, or
6. for the clarification and prevention of illegal or improper use.

(6) The administrator may temporarily restrict the use of resources or temporarily block individual user IDs to the extent necessary for troubleshooting, system administration and expansion, or for reasons of system security, to protect the user's own or other data, or to clarify and stop misuse. The affected users shall be informed immediately of the measures taken, to the extent that this is possible with reasonable effort. To clarify and prevent misuse in particular, the user may not be informed in advance. There must be actual and documented indications of misuse.

(7) The relevant statutory and legal provisions apply to the logging, inspection, and transmission of personal user data.

(8) The administrator may, in consultation with the Data Protection Officer, inspect the user's personal data to the extent necessary for troubleshooting, system administration and expansion, or for reasons of system security, to protect the user's own data or other data, or to clarify and prevent misuse. If possible, prior consent must be obtained from the affected user. In any case, the users concerned must be informed immediately of the measures taken. For the purpose of clarifying and preventing misuse or to the extent necessary for the prosecution of criminal offenses, the user may not be informed. There must be actual and documented indications of misuse or a criminal offense.

(9) The administrator shall undertake to document all measures in a comprehensible manner, in particular those pursuant to § 10 (5), (6), and (8).

§ 11
User Liability

(1) As part of the legal requirements, the user is liable for all damages incurred by TU Dresden due to misuse or illegal use of the IT infrastructure by the user or due to the user's culpable failure to comply with his/her duties under these regulations.

(2) The user shall also be liable for damages caused by third-party use as part of the access and use options made available to him/her, if he/she is responsible for this third-party use, particularly in the case of the transfer of a user ID to a third party.

(3) The user shall indemnify TU Dresden to the extent permitted by law against all claims asserted by third parties against the university for damages, injunctive relief, or otherwise based on the user's misuse or unlawful conduct.

§ 12
Sanctions for Misuse

(1) Users can be temporarily or permanently restricted in their use or banned completely if they
1. culpably violate these regulations (abusive conduct),
2. misuse the IT infrastructure of TU Dresden for criminal acts, or
3. cause detriment to TU Dresden through other unlawful user conduct.

(2) Measures under (1) shall be taken only after prior consultation. The person concerned shall be given the opportunity to comment.

(3) If there are factual indications that conduct pursuant to (1) has occurred, further use may be prohibited and blocked until the factual and legal situation has been clarified.

(4) Temporary restrictions on use shall be lifted as soon as proper use is again ensured.

(5) A permanent restriction on use or the complete banning of a user from further use can only be considered in the case of serious or repeated violations as defined in (1), even if proper conduct is not to be expected in the future. The restriction or ban may be lifted upon application or ex officio if the risk of recurrence no longer exists. This must be substantiated by the banned individual.

(6) Particular attention is drawn to the following offenses:
1. Data espionage (Section 202a German Criminal Code [StGB])
2. Phishing (Section 202b German Criminal Code [StGB])
3. Acts preparatory to data espionage and phishing (Section 202c German Criminal Code [StGB])
4. Data manipulation (Section 303a German Criminal Code [StGB])
5. Computer sabotage (Section 303b German Criminal Code [StGB])
6. Dissemination of pornography (Section 184 German Criminal Code [StGB])
7. Dissemination, procurement and possession of child pornography (Section 184b German Criminal Code [StGB])
8. Dissemination of propaganda material of unconstitutional organisations (Section 86 German Criminal Code [StGB])
9. Incitement of masses (Section 130 German Criminal Code [StGB])
10. Insult or defamation (Section 185 et seq. German Criminal Code [StGB])
11. Unlawful exploitation of copyrighted works (Section 106 et seq. German Copyright Act [UrhG])

(7) Furthermore, measures under labor law or disciplinary law may be taken against employees of TU Dresden.

(8) Criminal charges may be filed in the event of criminal conduct.

§ 13
Third Parties

Only in justified exceptional cases and taking into account the protection requirements of the information to be processed can third parties be commissioned to operate or support the IT infrastructure. This must be contractually agreed in consultation with the Information Security Unit.

Section 3: Use

§ 14
Purpose of Use and Admission to Use

(1) The establishment and operation of the IT infrastructure as well as admission to use the IT infrastructure shall be exclusively for the purposes of research, teaching and study, education and training as well as for the purposes of university administration and for the fulfillment of other tasks of TU Dresden.

(2) Admission to use is granted exclusively to members and affiliates of the closed user group. Guests pursuant to § 3 (2) can only be members of the closed user group for a limited period of time. A prerequisite for the admission of guests to the closed user group is determining the necessity of using the facilities and services specified in order to fulfill the guest's tasks at TU Dresden pursuant to § 14 (1).

(3) Unless otherwise specified by law, the use of the IT infrastructure pursuant to § 1 (1) for purposes other than those specified in § 14 (1) is permissible if it is minimal, does not hinder or disrupt the use of the IT infrastructure by other users, and does not impair the performance of official duties.

(4) In special cases, the responsible head of the structural unit may prohibit the use of the IT infrastructure pursuant to § 1 (1) of these regulations or parts thereof for other purposes. In cases of doubt, this is to be assessed by the Information Security Unit and a decision is to be made by the CDIO of TU Dresden.

(5) The use of hardware and software is only permitted if it is in line with the state of the art, and suitable and appropriate measures have been taken to protect the data processed on it. The competent administrator is responsible for the required check. If necessary, the administrator can restrict or completely prohibit use. In cases of doubt, he/she must contact the Information Security Unit directly. In such cases, the CDIO makes the final decision on the admission to use.

(6) The IT infrastructure may not be used to monitor the individual performance and conduct of TU Dresden's employees.

§ 15
User Administration

(1) A central user account in electronic form is created and administered for users at ZIH.

(2) For the administration of the central user account according to § 15 (1), the data may be processed which are necessary for the unambiguous identification of the user, for the proper operation of the IT infrastructure as well as for ensuring the proper course of business at TU Dresden. Data pursuant to § 15 (2) may be transmitted to information technology facilities and services only if it is established and proven in the individual case that the processing of such data is necessary for the proper operation of such facilities and services.

(3) If a user leaves, the central user account will be blocked after 14 days and after 15 months at the latest it will be deleted. Deletion also includes the data associated with the account.

(4) Users shall undertake to work exclusively with the user IDs which they have been authorized to use as part of the admission process. Each user must ensure that unauthorized persons are prevented from using his/her user account. This includes the careful choice of a password that is not easy to guess, in accordance with the ZIH password policy. Disclosure of the password is not permitted. The user is prohibited from obtaining and using third-party user IDs.

(5) Decentralized user administration is permitted if central user administration pursuant to § 15 (1) does not have the required functionalities and this is necessary to fulfill the tasks of the structural units. The same information security requirements apply to decentralized user administration as to the central user administration of ZIH. This must be submitted for authorization in advance via the Information Security Unit and the CDIO.

Section 4: Special Provisions for Naming Conventions, Email, and Web Applications

§ 16
Naming Conventions

(1) All end-user devices connected to the data network of TU Dresden should be given a unique name (host name) under the “tu-dresden.de” domain. ZIH administers this domain and its subdomains

(2) Unique host names are formed based on the pattern “hostname.structuralunit.tu-dresden.de”. For the “structural unit” section, the abbreviation of the School, faculty, department, Central University Administration (ZUV), or the Central Unit (ZE) can be used. The “hostname” section is defined by the user. Additional subdivision into subunits is possible.

(3) For all domains pursuant to § 16, the domain name service (DNS) shall be implemented by ZIH.

§ 17
Special Provisions for Email

(1) For purposes pursuant to § 14 (1), users shall undertake to use exclusively the email addresses which comply with the following naming conventions: for academic and non-academic staff: firstname.lastname[y]@tu-dresden.de and for students and guests: firstname.lastname[y]@mail.tu-dresden.de. Special characters are not permitted. Student assistants belong to the group of students (primary role). Existing decentralized email addresses are subject to grandfathering with regard to receiving authorization.

(2) Email addresses and central email distribution lists are set up and administered at ZIH, unless otherwise stipulated by law. Setting up and using email distribution lists is only permitted to the extent necessary to carry out the service or employment relationship, to implement organizational measures, and for training, testing, or academic purposes.

(3) If required, structure-related or function-related email addresses consisting of structuralunit@tu-dresden.de or function@tu-dresden.de can be assigned. These must be requested via the ZIH self-service portal.

(4) TU Dresden's incoming and outgoing email traffic is handled via the central gateway (mail relay) at ZIH. ZIH shall take all necessary measures for the proper operation of the mail relay.

(5) All incoming and outgoing email messages with invalid sender addresses are automatically rejected.

(6) A virus check is performed for all incoming and outgoing email messages. Emails containing viruses may be rejected.

(7) Each incoming email message is scored for spam using state-of-the-art technology before it is processed further. Users can configure the scoring themselves and specify whether the email messages that are then scored as spam are to be rejected or delivered as scored spam.

(8) Emails sent by academic and non-academic staff (from the @tu-dresden.de domain) must be signed with an electronic signature pursuant to § 3 (8) and must always be encrypted. It is not permitted to send particularly sensitive personal data or other data requiring a higher level of protection in unencrypted form by email.

(9) For official purposes, automated forwarding of incoming emails to mailboxes outside TU Dresden infrastructure is not permitted. Also, requesting that emails be automatically forwarded is not permissible.

(10) For academic purposes, the forwarding of email messages after the user has left is permitted upon request. ZIH provides a service (forwarding portal) for this purpose. Automated forwarding for other purposes or with other communications technology facilities or services is not permitted.

(11) At a minimum, the following shall be defined in the structural units by means of work instructions: Sender authorization, absence notifications, and substitution rules. ZIH provides the technical means to comply with this regulation.

§ 18
Guidelines for Websites

Structural units of TU Dresden are required to present themselves via the central TU Dresden website. Exceptions are permitted for collaboration projects with external partners as well as for special functional requirements, in which case the specifications of TU Dresden regarding corporate design as well as applicable legal regulations (especially regarding legal notice, data protection, and accessibility) must be observed. The Unit Web and Video provides advice and support on these requirements, and it cooperates with the Information Security Unit on data protection issues. The final decision on permissible exceptions is made by the CDIO, based on a decision proposal submitted by the Web and Video Unit.

Section 5: Information Security and Data Protection

§ 19
Principles

(1) The effort required to protect personal data or data requiring special protection in line with the state of the art must be proportionate to the intended protective purpose. The relevant statutory and legal provisions shall apply to the processing of personal data. In particular, the standards of the German Federal Office for Information Security (BSI) in the current version shall be authoritative for proof of the protective measures taken in accordance with (1).

(2) Information security is a performance characteristic of IT processes that must be assessed and implemented. For central IT processes, therefore, the need for protection in particular must be defined by the specialists, and for decentralized IT processes by the responsible superiors.

§ 20
Rights and Duties of the Information Security Unit

(1) The Information Security Unit must be involved in all projects that have a significant impact on information processing, as well as in the introduction of new applications and IT systems, in order to ensure that security and data protection aspects are adequately incorporated.

(2) The structural units must support the Information Security Unit in fulfilling its tasks. The Information Security Unit has a wide-ranging right to information on matters relevant to information security. To this end, the Information Security Unit must be provided in good time with all information that may be of significance for the fulfillment of its tasks. It may request any information necessary for its remit.

(3) The following tasks and rights in particular are assigned to the Information Security Unit:

1. Control and coordination of the information security process at TU Dresden,
2. Supporting the Extended University Executive Board and the CDIO in fulfilling information security responsibilities,
3. Conception, further development, and implementation of projects related to information security,
4. Conception and further development of internal university technical and organizational standards for information security,
5. Participation and coordination in the drafting of regulations and statutes related to information security,
6. Advising, supporting, and monitoring the structural units in implementing the legal requirements for information security,
7. Comprehensive control and evaluation of TU Dresden's IT infrastructure as well as procedures in which personal or other data requiring special protection are processed,
8. Initiating, reviewing, and confirming protection needs assessments and security concepts,
9. Investigation and evaluation of incidents relevant to security and data protection as well as establishment and operation of technical facilities of particular importance for information security,
10. Regular reporting to the CDIO on information security issues,

11. Binding statements on information security with the authorization of the CDIO,
12. Statements and notices to structural units with a duty to observe under their own responsibility,
13. Direct and timely information in the event of particular urgency and in individual cases to the CDIO and ZIH,
14. Planning, organizing, and conducting awareness and training measures on information security for members, affiliates, and guests of TU Dresden, and
15. Advice and support for members, affiliates, and guests of TU Dresden on information security issues.

§ 21
Reporting Requirements

In the event of a
1. reasonable suspicion or discovery of a violation of the provisions of these regulations,
2. reasonable suspicion or discovery of a loss of data,
3. reasonable suspicion or the discovery of unauthorized access to data,
4. reasonable suspicion or the discovery of a compromise of IT infrastructure (security incidents)

this must be reported immediately and directly to the Information Security Unit.

Section 6: Software and Hardware

§ 22
Hardware and Software Procurement, Use, and Software Licensing

(1) The procurement of hardware and software is defined in TU Dresden's procurement policy (with the exception of the Carl Gustav Carus Faculty of Medicine).

(2) All software products to be procured for official use at TU Dresden shall be applied for via ZIH in consultation with the Directorate Planning and Organization. The purchase of micro software (apps) under your own responsibility is permitted if it has been verified prior to procurement that the software is not included in existing campus contracts and sufficient funds are available. Members and guests of TU Dresden with their own cost center are entitled to purchase, provided that the contractual terms and conditions of the manufacturer permit it.

(3) The strategic and technical responsibility of campus contracts and framework agreements is generally the responsibility of the CDIO, the Planning and Organisation Directorate, and ZIH.

(4) The disposal of hardware and software is carried out according to the rules of TU Dresden's inventory regulations. In doing so, the stipulations of BSI Grundschutz (BSI basic protection) for the deletion of stored data must be observed.

(5) Users are entitled to use the software only for TU Dresden in the quantity licensed and only for work in research and teaching on the computers in their areas of responsibility. For other, e.g., industrial, commercial, or profit-making purposes, the licensing terms or contracts for the respective software product of the manufacturer shall apply.

(6) Private use of software acquired for official purposes requires that this form of use is expressly approved in contractual or licensing provisions on the part of TU Dresden and by the manufacturer.

(7) The use of privately purchased software for business purposes must be covered by the manufacturer's licensing terms and requires the approval of the responsible superior.

(8) Student licenses are reserved for use by students. Exceptions (use by other groups of persons) are only possible with the consent of the software manufacturer.

(9) Depending on the software contract, the user is granted the right of use for an unlimited or limited period of time. If use is limited in time, the software must be uninstalled at the end of this period of use without being requested to do so by ZIH.

(10) If the user leaves the employment or service relationship with TU Dresden, the provided hardware and all licenses are to be returned to the structural unit.

(11) In the event of a license check (audit) by the software manufacturer, ZIH is authorized to perform a TU Dresden-wide check in coordination with the Information Security Unit.

(12) Audits requested by software manufacturers regarding the use of the software are to be coordinated with the Information Security Unit of TU Dresden. After informing the superior, the administrator is authorized to provide the information required for the evaluations.

(13) When using software, documentation, and other data, the legal requirements, in particular those relating to copyright protection and accessibility, must be complied with and the licensing terms under which software, documentation, and data are made available must be observed.

Section 7: IT Emergency Management

§ 23
Entry into Force/Expiry of IT Emergency Management

(1) The CDIO is responsible for the basic determination and duration of IT emergency management and the emergency plans, exceptions, and notification chains that go into effect as a result. The Extended University Executive Board shall be informed concurrently.

(2) If an individual structural unit is affected by an IT emergency, determination of this is the responsibility of the competent head of the structural unit in consultation with the Information Security Unit.

Section 8: Final Provisions

§ 24
Entry into Force/Expiry

These regulations come into force on the day after publication in the official announcements of Technische Universität Dresden. Thus, the Regulations for the Information Technology Facilities and Services and for Information Security at TU Dresden (IT Regulations) of May 7, 2019 (official announcements of TU Dresden No. 08/2019 of May 17, 2019, p. 592) shall cease to be in force.

Dresden, dated February 18, 2021

The Rector
of Technische Universität Dresden

Prof. Dr. Ursula M. Staudinger