Technische Universität Braunschweig

Contents

Information Security Regulations for TU Braunschweig

Informationssicherheitsordnung der TU Braunschweig

Preamble

These Regulations govern the competences and responsibilities as well as cooperation in the university-wide information security process.[1] The aim of the Information Security Regulations (Informationssicherheitsordnung) is not only to fulfil the existing legal requirements, but also to protect TU Braunschweig from damage as far as possible. The development and updating of the Information Security Regulations (Informationssicherheitsordnung) must be oriented on the legally defined tasks of the university as well as its mandate to safeguard academic freedom. However, this can only be achieved through a continuous information security process within regulated structures of responsibility. In establishing and further developing the information security process, these Regulations are guided by general requirements for proper IT operations which are summarised in the “Minimum Requirements of the Courts of Audit of the Federation and the Laender for the Use of Information Technology”.[2] These minimum requirements for IT operations refer to generally accepted legal and technical standards. In the area of technical implementation of information security, these are, for example, the “Basic Protection Compendium (Grundschutz-Kompendium)”[3] of the Federal Office for Information Security (Bundesamts für Sicherheit in der Informationstechnik (BSI)), which is based on the largely equivalent standards of the ISO 2700x series, the “Basic Protection Profile for Universities Grundschutzprofil für Hochschulen)”[4] developed by the Association of University Computing Centres in Germany (“Zentren für Kommunikation und Informationsverarbeitung e.V.” (ZKI)) and other established sources that reflect the current status in their respective versions.The legal foundations of these Regulations are:

- The obligation to create appropriate minimum standards in accordance with the “Guideline for Ensuring Information Security” (Leitlinie zur Gewährung der Informationssicherheit (ISLL)) of the State of Lower Saxony
- § 37(1) in conjunction with § 3 NHG.

These Regulations use the aforementioned norms to derive the guidelines for information security and IT security applicable at TU Braunschweig.

---

[1] These Regulations focus on the information technology aspects of information security. Other aspects such as physical security and organisational security must also be developed and observed in other areas of the university (e.g., building management, process development, work processes in the organisational units).
[2] https://www.bundesrechnungshof.de/de/veroeffentlichungen/produkte/weitere/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informationstechnik/mindestanforderungen-der-rechnungshoefe-des-bundes-und-der-laender-zum-einsatz-der-informations-und-kommunikationstechnik/@@download/file [last accessed: 24 June 2021]
[3] BSI Basic Protection Compendium (Grundschutz-Kompendium) https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html [last accessed: 8 July 2021]
[4] ZKI Basic Protection Profile for Universities (Grundschutzprofil für Hochschulen): Primary document and commentary elements https://www.zki.de/fileadmin/user_upload/Downloads/IT-Grundschutz-Profil_fuer_Hochschulen_V1_0.pdf and https://www.zki.de/fileadmin/user_upload/Downloads/IT-Grundschutz-Profil_fuer_Hochschulen_Bausteinkommentierungen_V1_0.pdf [last accessed: 8 July 2021]

§ 1 Subject of the Regulations

The subject of these Regulations is the definition of the responsibility structures required for realising a university-wide information security process,[5] an allocation of tasks as well as the definition of the cooperation of those involved. These Regulations are supplemented in the technical field by the following regulations:

(1) Information Technology Usage Regulations (Nutzungsordnung zur Informationstechnologie) at Technische Universität Braunschweig,
(2) Information Services Regulations (Informationsdienste-Ordnung) at Technische Universität Braunschweig,
(3) Guidelines for information security and IT security on individual topics and
(4) Existing and future service agreements on information security and the use of technical devices.

§ 2 Scope of application

(1) The scope of these Regulations extends to all organisational units of TU Braunschweig in accordance with § 4 of the University Charter Grundordnung of TU Braunschweig (in particular the bodies in accordance with §§ 3 and 4 of the Charter (Grundordnung)), to the entire IT infrastructure for which TU Braunschweig is responsible, including all centrally and decentrally operated IT systems, as well as including all externally operated and commissioned systems, taking into account the processes which these systems serve.
(2) The provisions of these Regulations and the resulting guidelines shall be observed in agreements and contracts with affiliated institutes and non-university institutions that are directly connected to the university network or are co-users of the German Research Network (Deutsches Forschungsnetz (DFN)) via this university network.

§ 3 Participants in the information security process

The overall responsibility for the information security process lies with the university management.[6] It appoints the following bodies and functionaries as participants in the information security process:

(1) The CIO Board (CIOB),
(2) The Chief Information Security Officer (CISO) as the person responsible for information security appointed by the university management,[7]
(3) IT Security Board (IT-SB),
(4) An operational Information Security Management Team (ISMT) (Head: CISO),
(5) Decentralised information security officers (DISB) of the decentralised organisational units,
(6) The Gauß IT Centre (GITZ),
(7) University Library (UB)
(8) The management of the university's organisational units. These are given responsibility for compliance with the standards for their area.

[5] Always related to electronically supported information processing.
[6] § 37(1) Lower Saxony Higher Education Act (Niedersächsisches Hochschulgesetz (NHG))
[7] The terms "Central Information Security Officer (ISB)" or "Information Security Officer (ISB)," "Chief Information Security Officer (CISO)," "person in the role of CISO" as well as "commissioned person for information security" are equivalent and are used synonymously.

The designated participants work together in a division of labour to comply with the information security standards at TU Braunschweig.
The CIO Board (CIOB) of TU Braunschweig shall be designated as the participating governing body of the university at the time these Regulations come into force.

§ 4 Appointment of the participants

(1) The university management shall appoint a CISO as the person responsible for the conception, implementation and monitoring of the information security process. The Vice President in charge of information security[8] shall be designated as the deputy; in the absence of both the CISO and the Vice President in charge of the topic, the Vice President for Human Resources, Finance and University Construction (HVP) shall act as the deputy.
(2) The university management shall establish the IT-SB and appoint the CISO as the leading person.
(3) The IT-SB shall appoint the ISMT. The ISMT is an operational group and is led by the CISO.
(4) All organisational units that use information technology shall appoint one person as DISB[9] and another person as deputy. Several organisational units can use a common DISB together.
(5) All information-processing systems and all users are to be assigned to one DISB each. This assignment shall be documented. If no self-assignment is made, the university management may also decide on corresponding assignments ("fall-back solution")
(6) In the faculties, the DISB and deputies shall be assigned in such a way that all information-processing systems operated there and all IT users are assigned accordingly. The faculties shall appoint a DISB as well as a deputy at the faculty level. If further DISB are then appointed at the institute level, they shall assist the DISB appointed at the faculty level.
(7) The DISB appointed for the GITZ shall also be responsible for the information security matters of the central administration.
(8) The student body shall be involved in the information security process via a person to be delegated by the student parliament as an advisory member of the IT-SB.
(9) When appointing the DISB and ISMT, care must be taken to ensure continuity in terms of personnel. If possible, the participants should belong to the full-time staff of TU Braunschweig.
(10) The operational group of the ISMT shall consist of employees assigned in whole or in part to the CISO and the persons listed in § 5. Additional persons from other organisational units may be assigned to the ISMT. The ISMT supports the work of the CISO.

[8] As of the point in time these Regulations were passed: Vice President for Digitalisation and Technology Transfer (VP-DT)

[9] In the following, the acronym DISB is also used for a person or persons who have assumed the role of a decentralised information security officer for a (decentralised) organisational unit.

§ 5 Composition of the IT Security Board (IT-SB) / Appointment of Information Security Officers

(1) The members of the IT-SB shall be appointed by the Executive Committee (see Appendix). The IT-SB is managed by the CISO.

(2) The IT-SB shall establish the Information Security Management Team (ISMT) as an operational group that supports the CISO person in operational business. Permanent members are:
- CISO as chairperson,
- the DISB of the faculties,
- a person designated by the management of the Gauss IT Centre,
- a person designated by the management of the University Library,
- the employees assigned to the CISO (information security management, staff unit CISO).

(3) The IT-SB and ISMT are to seek the advice of internal and external experts as required (e.g., for sub-areas of information security or IT operations).

§ 6 Tasks of the persons involved in the information security process

(1) Maintaining information security is the responsibility of the management in whose area the respective information is processed, including the technical systems used for this purpose as well as the design of the information-processing processes. It includes safeguarding technical systems, designing information-processing processes, and instructing and training the persons carrying out these processes. The task can be transferred to this extent to a (decentralised) information security officer. This does not release the management of the university as a whole or the management of the respective organisational unit from their overall responsibility for information security in their respective area.

(2) The CIOB, as the highest advisory and supervisory body in matters of information security, decides on the recommendations for action and proposes the strategic information security guidelines for TU Braunschweig. The Executive Committee adopts the Strategic Information Security Guidelines and these Regulations and other recommendations for action prepared by the CIOB taking into account the recommendations from the IT-SB and agreed with the bodies involved. The CIOB, with input from the IT-SB, develops the associated technical guidelines from the Guidelines and these Regulations and brings them into force. The CIOB submits the information security report to be prepared annually by the IT-SB to the Executive Committee. The CIOB addresses information security concerns at least once per quarter or as requested by the CISO.

(3) The IT-SB forms the central advisory and control body for the University in matters of information security for the time between the meetings of the CIOB. It draws up the central technical framework guidelines for the university's information security. The IT-SB advises the CIOB and the Executive Committee on all information security and risk assessment issues. The IT-SB meets regularly six times a year or at the request of the CISO.

(4) The CISO
   a. is responsible for monitoring the implementation of the information security regulations (Informationssicherheitsordnung) and guidelines at the university (Richtlinien der Informationssicherheit) and is supported in this by the IT-SB; this does not relieve the university management of its responsibility to ensure adequate information security,
   b. establishes, operates, and develops an information security management system (ISMS) in accordance with changing requirements,
   c. is the person to be addressed internally and externally in all information security-related matters,
   d. coordinates the investigation and documentation of information security-related incidents and develops an information security training and development plan,
   e. is appointed in accordance with the BSI's[10] basic protection[11] guidelines,
   f. reports directly to the responsible governing body (CIOB) and has direct access to the university management if required; it is not permissible for the CISO to also be the DPO or an IT manager (e.g., responsible vice president, management of the Gauss IT Centre),
   g. is to be informed on all topics relevant to information security in all organisational units without being asked,
   h. has the right to make oral and written statements to the university management in all matters of information security,
   i. has access – if necessary after prior consultation with the DPO – to all affected IT systems at TU Braunschweig in order to carry out monitoring and advisory tasks,
   j. has access rights to all rooms in which information technology is used,
   k. shall be supported by the management level in the performance of the duties arising from this order by making available adequate financial, human, and other resources and shall ensure their own appropriate education and training,
   l. is not bound by instructions from the university management in the professional function as CISO in order to avoid conflicts of interest.

(5) The ISMT is the operational basis for practically implementing the information security process across the university and for discussing experiences.

(6) The ISMT supports the CISO and the DISB in their practical work. This operational group meets as needed and determines its own meeting frequency. The ISMT is headed by the CISO.

(7) The DISB shall conduct the information security process and training of employees in their organisational units on information security. The managers are responsible for decentralised IT operations and support the DISB in the implementation and execution of the information security process.

(8) The DISB are not bound to instructions from their superiors with regard to their reporting duties to the CISO. The DISB also provide their reports to the management of the organisational units concerned.

(9) The designation of the DISB does not relieve the management of the organisational units of their responsibility for information security in their area.

---

[10] Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
[11] BSI Basic Protection Compendium and Implementation Guidelines https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html and https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Umsetzungshinweise/umsetzungshinweise_node.html [last accessed: July 9, 2021]

(10) Regarding all structural planning, procedures and decisions related to information security, the DISB are required to keep the CISO appropriately informed. These include, in particular, plans and decisions that are related to the information security of processes.
(11) The Gauss IT Centre supports the DISB, the ISMT, the IT-SB, and the CISO in technical matters and in the practical implementation of necessary measures. Appropriate resources for this are to be taken into account in the annual budget negotiations of the GITZ.
(12) The organisational units of the University are obligated to involve the responsible DISB and the CISO in advance in all relevant plans, procedures and decisions relating to information security, including plans for new services or information-processing systems.
(13) Those involved in the information security process cooperate in all matters of information security, provide the necessary information for this purpose and regulate the communication and decision-making channels both among themselves and in relation to third parties. In this context, in particular the aspect of urgency required in crisis situations must be taken into account.

§ 7 Implementation of the information security process

(1) The CISO, together with the IT-SB and supported by the ISMT, shall introduce a university-wide information and communication system. All those involved in the information security process are in contact via this system.
(2) The DISB are obliged to obtain up-to-date security-related information for the area under their responsibility, unless this information is obtained and distributed centrally, and are supported in this by the CISO and ISMT. The DISB shall arrange for the necessary information security measures in their area to avert a threat. To this end, they must be provided by the management of their organisational unit with the necessary competences and authority as well as material resources. If measures that extend beyond a single organisational unit are necessary to avert a threat, the CISO is entitled to order these measures directly. If an organisational unit does not take action within a timeframe appropriate to the threat, the CISO is entitled to order appropriate security measures directly, and the organisational unit must be informed of this in a timely manner. In any case of averting threats, the CISO shall be involved.
(3) Those involved in the information security process shall inform each other as quickly as possible, comprehensively and completely about security-relevant incidents. The CISO must be informed of every incident.
(4) The CISO is authorised to obtain all relevant information that arises during the handling of an IT security incident and in the context of an intervention (§ 8) in the individual facilities.
(5) The IT-SB shall continuously develop the framework guidelines. The participants involved in the information security process may submit proposals to the IT-SB for this purpose.

§ 8 Intervention

(1) In the event of a significant breach of the Information Security Regulations (Informationssicherheitsordnung) or the University's Information Security Guidelines (Richtlinien der Informationssicherheit), as well as in the event of acute threat situations, the CISO may order the immediate, temporary shutdown of the affected IT system, temporarily exclude the responsible users from using the information technology and take and order other necessary measures. The CISO must inform the DISB of the incident as soon as possible.

(2) In the event of a significant breach of the Information Security Regulations (Informationssicherheitsordnung) or the University's Information Security Guidelines (Richtlinien der Informationssicherheit) at a decentral location, the responsible DISB may order the immediate, temporary shutdown of the affected IT system, temporarily exclude the responsible users from using the information technology and take and order other necessary measures. The responsible DISB must inform the CISO and the IT-SB of the incident as soon as possible.

(3) In the event of anomalies and especially in the event of imminent danger, the Gauss IT Centre may temporarily block network connections or take other measures insofar as these are suitable for averting foreseeable damage to the university. The Gauss IT Centre must inform the CISO, the IT-SB and the DISB concerned of the process as soon as possible.

(4) The return to service of temporarily suspended information systems or the reversal of other actions taken shall be subject to the detailed review and approval of the DISB and the agreement of the CISO.

(5) After consultation with the IT-SB, the CISO may lift the ban of a user who has been temporarily banned from the use of the information technology.

(6) The order in this list does not specify any order for the measures to be taken.

(7) The IT-SB shall define the IT services for which the CISO shall coordinate the preparation of contingency plans. They contain instructions for action in dangerous situations and in the event of incidents and are divided into a notification plan that is generally accessible to the university public and a detailed emergency concept for official use as well as specifications as to the cases in which TU-wide crisis management is necessary. The details on the enactment and implementation of the emergency plans shall be regulated by the CIOB on the proposal of the IT-SB; the regulations shall be documented in a suitable format for emergency planning and made available to the respective organisational units concerned.

§ 9 Equality clause

Status and function designations under these Regulations make no reference to the gender of the persons filling them.

§ 10 Entry into force

These Information Security Regulations (Informationssicherheitsordnung) shall enter into force on the day following their adoption by the Senate. At the same time, the IT Security Regulations (Ordnung zur IT-Sicherheit) (public university announcement of July 7, 2003 [TU Gazette No. 272]) shall cease to apply.

Passed by the Senate at the meeting on March 16, 2022

Appendix

Composition of the IT-SB according to the decision of the Executive Committee from May 12, 2021: Setting up and appointing the IT Security Board (IT-SB)

On § 5:
The members of the IT-SB:

- Chief Information Security Officer (CISO),
- Vice President for Digitalisation and Technology Transfer (VP-DT),
- Vice President for Human Resources, Finance and University Construction (HVP),
- Head of the Gauß IT Centre.

The IT-SB is headed by the CISO.

The advisory members of the IT-SB:

- Data Protection Officer (DPO),
- Data Protection Management Officer,
- Staff Council Representative,
- Chair of IT Multi-Project Management Board (IT-MMB),
- Chair of IT User Board (IT-UB),
- Decentralised Information Security Officers (DISB),
- Head of the Project Management Office (PMO).