Technische Universität Braunschweig

Contents

1 Information security as a challenge 1
2 Strategic task of the university management 2
2.1 Definition of "information security" in the context of higher education 3
2.1.1 Definition of "information security" according to DIN/ISO/IEC 27000:2017 3
2.1.1.1 Definitions and core properties 4

Strategic Guidelines for Information Security at TU Braunschweig

1 Information security as a challenge

Science requires trust. This applies both to research and teaching and, building on this, when transferring knowledge to society. All of these are core tasks of TU Braunschweig. Information security is an indispensable prerequisite for the fulfilment of these core tasks by all participating organisational units of TU Braunschweig.

Universities, like other organisations, are exposed to growing threats and risks to information and knowledge. These dangers and risks affect the core tasks of teaching, research and knowledge transfer, and thus also central and decentralised administration in a specific way, especially with regard to:

- Loss of integrity and availability of research and personal data, including in teaching and administration,
- Compromising the personal data of all university members and
- Loss of confidentiality of data within collaborative relationships, for example through espionage.

The main sources of danger for the reduction or loss of IT security include, for example (at the time these guidelines were adopted):

- Attempts to obtain personal data via fake websites, emails or short messages ("phishing"): Phishing attacks can target log-in data for research purposes, for student examinations or for administrative management tools. Phishing is also a real danger in connection with espionage activities.
- Infection and locking of computers of TU members inside and outside the TU network in order to subsequently demand money for the unlocking or non-disclosure of sensitive data ("ransomware"). If, for example, a central university computer is successfully infected or blocked, research, teaching, study and administrative activities could come to an abrupt standstill for several months and sensitive data could also be lost. Similar consequences can occur if external parties use the university infrastructure for botnets.
- The deliberate or unnoticed transfer of access authorisations to parts of the IT infrastructure to unauthorised persons, which subsequently prevents the availability of data or its protection.
- The use or processing of university-related data on end devices that are not protected against unauthorised access in accordance with the state of the art.

Universities are particularly vulnerable. Contributing factors include:

- The worldwide cooperation of the most diverse organisational units (OUs) within TU Braunschweig or with external partners for scientific exchange,
- The extensive autonomy of many OUs,
- The project character of activities and processes,
- A comparatively high staff turnover,
- The different status groups with their various roles and rights and heterogeneous awareness levels as well as
- The rapid development cycles of information technology.

Establishing and maintaining information security therefore represent a significant challenge[1] and ongoing task for higher education institutions.

2 Strategic task of the university management

In the scientific environment, the term "information security" primarily targets the aspects of integrity, confidentiality as well as availability and exchange of information. The focus is on electronically stored data, including the associated processing procedures (including manual procedures). Nevertheless, the protection of analogue data is also a subject of information security.
Information security differs from IT security in that the good to be protected, “information," and the associated information-processing procedures are placed in the foreground of risk assessment and treatment. IT security considers the technical aspects and is therefore a part of information security.
Anchoring information security as an aspect of process quality in the university is legally required and thus also an organisational task within the framework of the governance structure and institutional awareness. The university management must actively take up these aspects for all areas of activity. The resulting organisational and cultural dimensions can only be brought together, evaluated and addressed

[1] See https://www.hrk.de/positionen/gesamtliste-beschluesse/beschluss/detail/informationssicherheit-als-strategische-aufgabe-der-hochschulleitung/ [last accessed: June 24, 2021].

in their entirety by the university management. Information security is therefore an original strategic task of the university management and must be embedded in all processes of the university. The scope and depth of the protective measures must always be set in relation to the security gain achieved and the value of the goods to be protected, as only in this way can the need for security and the freedom of research, teaching and an efficient transfer of technology and knowledge be reconciled in the long term. The university management's responsibility for information security extends in particular to creating and continuously developing functioning structures for planning, implementing, reviewing and improving information security in order to be able to adequately counter current developments of different threat situations. In these structures, the specialist side and the operators of the information technology infrastructure must work together and the relationships to and between the roles of data protection, information security, the legal department, the Executive Committee, the press office and the incident reporting offices must be regulated. Sufficient resources must be made available to achieve an adequate level of security.
The perception of responsibility for information security is - as with the topic of data protection - outwardly expressed primarily through

- staff members who are explicitly designated as responsible for procedures,
- regulated reporting channels and the existence of a response team,
- regulated risk management,
- the documentation of a security strategy and measures in the form of guidelines and an information security concept as well as
- a continuous improvement process.

Reporting, response and documentation obligations as well as risk management must be implemented and documented in a coordinated manner for information security, IT security and data protection. The level of security actually achieved depends to a large extent on the consideration of information security when redesigning and reorganising all business processes and activities, as well as on the awareness of information security within the university, the existing expertise in information security and IT security and the successful interaction of the structures described above.

2.1 Definition of "information security" in the context of higher education

The term *information security* is defined by various standardisation organisations (see below for the ISO/IEC/DIN definition), but these definitions usually focus on a general corporate environment. For science and its working methods - and universities in particular -, a science-related interpretation is required in terms of objectives and measures.

2.1.1 Definition of "information security" according to DIN/ISO/IEC 27000:2017[2]

"Information security: The preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved."

[2] https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:269670716(ISO 27001, version 2017 is the currently valid standard) [last accessed: June 24, 2021]

2.1.1.1 Definitions and core properties[3]

Information security is a complex, abstract construct for which no uniform definition exists. For example, the German Federal Office for Information Security (BSI) describes information security based on the ISO 27001 standard as the protection of confidentiality, integrity and availability of the information.[4] Similarly, the U.S. National Institute of Standards and Technology (NIST) defines information security as ensuring "the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability."[5] Although definitions of information security within the scientific community often include other aspects such as authenticity and verifiability,[6] these definitions mostly have in common that they describe the protection of the three core properties of information security, i.e. confidentiality, integrity and availability.[7] These terms imply the following:

- Confidentiality: the protection of confidential information from unauthorised access.
- Integrity: the protection of data and information systems against unauthorised modification and deletion of information.
- Availability: ensuring timely and reliable access to information and information systems.

Information security requires the application and management of appropriate security measures, taking into account a wide range of threats, with the aim of ensuring continuous operation[8] at an appropriate level and minimising disruption from information security incidents. Information security is achieved through the implementation of a suitable catalogue of measures developed as part of an operational risk management process. These measures must be defined, implemented, monitored, reviewed and improved where necessary to ensure that TU Braunschweig's specific information security and business objectives are met. They are controlled with the help of an information security management system (ISMS). The ISMS in turn includes policies, processes, procedures, organisational structures, software and hardware to protect identified information assets. In principle, the aim should be to integrate information security measures as seamlessly as possible into the organisation's business processes. Data must meet both quality assurance and information security requirements. In addition, TU Braunschweig operates in a global environment and is in open exchange with society. This results in a balancing act between different goals:

- The postulate of *openness*, of digital and analogue research processes, methods and results (Open Access, Open Science, Open Data) and of teaching and learning content (Open Educational Resources) implies that the protection goals of *integrity* and *availability* have a particularly high priority.

---

[3] https://enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/uebergreifendes/Kontext-und-Grundlagen/IT-Recht/informationssicherheit [last accessed: June 24, 2021]
[4] Federal Office for Information Security, Grundschutz-Kompendium 2020, p. 15, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf%3F__blob%3DpublicationFile%26v%3D6[last accessed July 8, 2021]
[5] FEDERAL INFORMATION SECURITY MODERNIZATION ACT https://www.cisa.gov/federal-information-security-modernization-act[last accessed: July 8, 2021]
[6] Gordon, Lawrence A.; Loeb, Martin P. The economics of information security investment. ACM Transactions on Information and System Security 5(2002), No. 4, p. 438-457
[7] Dehling, Tobias; Sunyaev, Ali. Secure Provision of Patient-Centered Health Information Technology Services in Public Networks—Leveraging Security and Privacy Features Provided by the German Nationwide Health Information Technology Infrastructure. Electronic Markets 24(2014), No. 2, p. 89–99
[8] In the security context, this is usually referred to as "business continuity".

- The postulate of *confidentiality* arises from the need for protected areas for scientific cooperation and not least from scientific competition and cooperation with partners from industry (especially in the context of contract research), confidentiality requirements for administration as well as the requirements of personal data protection according to the GDPR in all areas of the university.

The necessary considerations with regard to formulating protection goals and risk assessment must be worked out by the responsible committees of TU Braunschweig. The implementation must then be decided on by the university management within the framework of the applicable laws.
In contrast to IT security, information security also includes non-information technology systems and ensures that non-digital systems are also protected through appropriate operational organisation and specifications. Thus, information security goes further than IT security, as it includes information technology systems, non-information technology systems, physical security (including building security) and the organisation. It implicitly takes into account media breaks between digital and analogue parts of processes.
Accordingly, the field of information security can only be dealt with through cooperation among the specialist side (research, teaching, knowledge transfer, administration) and the information system side (computing centre, library, data protection), physical security represented by building management and the definition of organisational processes. In particular, developing framework conditions for process transparency as well as rules of conduct in the form of guidelines and directives are designed and supported by the university. Consideration of the processes for which the existing IT technology is used is an elementary component of information security and can only be ensured by the process managers. In doing so, preparing risk assessments and taking risk decisions must be integrated into the university's processes. The task of anchoring information security as an aspect of process quality in the university organisation is the joint responsibility of the central and decentralised organisational units. Information security is not only legally required, it is also part of an overarching organisational task within the framework of institutional awareness and the further development of governance structures and processes to which all university members must contribute.

Executive Committee resolution of February 9, 2022, confirmation by the Senate on February 16, 2022