Information Security Guideline of the University of Bayreuth,

version date: 10 March 2022

Preamble

For the University of Bayreuth, information and communication technology is of central importance for the fulfilment of tasks in research and teaching. The spectrum of IT applications includes the operation of facilities, the performance of tests and experiments, scientific applications and simulations, teaching, work in administration and central services, and communication with external partners and clients.

Security in information technology as well as compliance with data protection and legal regulations are a fundamental prerequisite for a functioning infrastructure at the university. It is the responsibility of all university institutes and users of the IT infrastructure to ensure this.

The goal is to protect information and data in an appropriate manner so that

1. confidentiality is protected in an appropriate manner and knowledge can only be obtained by authorized persons,
2. integrity is ensured by their accuracy and completeness,
3. availability is guaranteed so that they can be used by authorized persons at the desired time,
4. legal obligations can be fulfilled.

The Information Security Guideline supplements the Regulations for the Information Processing Infrastructure of the University of Bayreuth (IT Regulations) dated 30 November 2018, as amended.

Information security at the University of Bayreuth is based on the basic understanding of the German Federal Office for Information Security (BSI) regarding information security.

§ 1

Subject of the Information Security Guideline and Definitions

The present guideline defines responsibilities, duties and tasks as well as regulations on funding in the area of information security.
[2]For the purposes of the present guideline

1. "Information security”:
   Ensuring confidentiality, integrity and availability of information processing and storage technical and non-technical systems.
2. "IT infrastructure”:
   The totality of the University's hardware, applications, and building facilities used for information processing.
3. "IT System”:
   The functional unit of hardware and software that collects, records, prepares, uses, stores, transmits, programmatically processes, internally displays, outputs and retrieves data.
4. "Information Security Process”:
   The set of procedures that have the goal of integrating information security into all of the University's operations to ensure constant development and improvement of information security.

§ 2

Scope

The information security guideline applies to all persons and systems using the IT infrastructure of the University of Bayreuth.

§ 3

Basic responsibilities

(1) All users of the IT systems connected to the IT infrastructure of the University of Bayreuth are obligated to work towards information security and to take the necessary measures to achieve this.

(2) Responsibility for information security basically follows the responsibilities for IT systems.

(3) [1]All users are responsible for reporting events that affect or could affect information security to the IT Service Centre immediately after becoming aware of them. [2]The IT Service Centre then notifies the Information Security Officer (ISB).

§ 4

Stakeholders in the information security process and their tasks

(1) University Governing Board

[1]The overall responsibility for ensuring information security and compliance with the information security process at the University of Bayreuth lies with the University Governing Board.

[2]The Vice President for Digitization, Innovation & Sustainability, as a member of the University Governing Board, shall perform the coordination tasks in the area of information security affecting the university as a whole after consultation with the Information Security Officer (ISB).

[3]The Chief Information Officer (CIO) is either the Vice President for Digitalization, Innovation & Sustainability or a university lecturer.[4]He or she develops the IT strategic goals and implementation concepts for a common IT management of the University of Bayreuth in a continuous progress process with the participation of the Information Security Officer (ISB).

(2) Presidential Advisory Committee for Information & Communication Technology (PK IKT)

[1]The PK IKT develops strategic proposals for the area of information and communication technology as a basis for decision-making by the University Governing Board. [2]Results of the Information Security Working Group, which is subordinate to the PK IKT, are reported to the PK IKT. [3]Once resolved, these are forwarded to the University Governing Board for approval or enactment, as appropriate.

(3) Information Security Working Group (AK Informationssicherheit)

[1]The Information Security Working Group prepares strategic objectives and decisions in the area of information security for PK IKT. [2]The working group initiates, steers and coordinates the information security process with the participation of the ISB. [3]This includes
among other things, all topics relating to information security.

(4) Information Security Officer (ISB)

[1]The ISB is appointed by the University Governing Board. [2]The ISB is a permanent member of the PK IKT and the Information Security Working Group.

[3]The ISB has a right to information and a right to make proposals.

[4]The ISB's right to information is exercised, among other things, through participation in university committees and inclusion in their information distribution lists. ^In addition, there is an active right to information for the ISB. [6] This person can access the minutes of the University Governing Board, University Council, Senate, faculty councils and minutes of the IT Service Centre, etc. if they relate to the topics of IT infrastructure and information security.

[7] The ISB's right to make proposals serves to make his or her own suggestions regarding information security to all parties and bodies mentioned under § 4 as well as to users.

The ISB is to be involved in all projects that have a significant impact on the security aspects of information processing.

[9]The duties of the ISB include investigating information security incidents and preparing reports on the state of information security.

[10]In his or her duties relating to information security, the ISB shall be bound only by directives of the University Governing Board.

[11]The University shall ensure that the ISB is relieved of this/her other duties to the extent necessary for his/her information security responsibilities and is adequately resourced.

(5) **Head of IT Service Centre (L-ITS)**

[1]The L-ITS is responsible for the information security of the IT infrastructure operated by the IT Service Centre and documents the security measures implemented in the IT service centre.[2]He or she is a permanent member of the PK IKT and the Information Security Working Group. [3]He or she shall carry out the resolutions of the University Governing Board.

(6) **Person responsible for IT systems**

[1]Those responsible for IT systems are entitled to take further measures within their area in addition to the university-wide information security measures. [2]If there is a potential impact on the University's IT infrastructure, coordination with the IT Service is required. [3]The measures taken independently must be documented.

§ 5
Hazard intervention

[1]the IT Service Centre has the right to immediately take necessary defensive measures in case of imminent danger. [2]The principle of proportionality of means shall be observed in the measures to be taken. [3]The measures should be taken in such a way that the affected user is informed in advance if at all possible. [4]The affected user, the management of the affected facility and the ISB shall be informed immediately of the incident and the measures taken.

[5]In the event of an incident that is classified by a person responsible for an IT system as a potential information security risk event, he or she is obligated to take appropriate defense measures and to inform the IT Service Centre and the ISB of the event and the measures taken as soon as possible.

[6]The security measures are lifted after sufficient information security measures have been implemented.

§ 6

Preventive measures

[1]Preventive measures are necessary to ensure information security. [2]Suitable technical and organizational measures are to be used to identify and contain risks and to detect attacks on information security at an early stage. [3]Interdepartmental measures are coordinated in the Information Security Working Group. [4]The Information Security Working Group may propose preventive measures. ^The implementation of preventive measures is the responsibility of the respective IT system operator.

§ 7

Financing

[1]The human and financial resources of the central information security operations are funded from central university resources.

[2]The ISB will be provided with a budget for further education and training costs from central funds.

[3]Further information security measures will be financed by the subunit that initiates and is responsible for these measures.

§ 8

Update provisions to maintain and further develop the information security process

The Information Security Working Group is tasked with continuously reviewing and developing the information security strategy and the effectiveness of the previous organizational form, measures and processes for information security and reporting on this at least every two years.

§ 9

Effective date

'This Information Security Guideline of the University of Bayreuth shall become effective on 11 March 2022. [2]It replaces the previous information security guideline of the University of Bayreuth, which was adopted in the meeting of the University Governing Board on 24.09.2019.

Resolution of the University Governing Board dated 8 February 2022