Trier University
of Applied Sciences

HOCHSCHULE TRIER

Information Security Guideline

Trier University of Applied Sciences

Content

Measure:	Guideline according to BSI IT-Grundschutz ISMS 1.A3
Scope:	All facilities of the university
Responsible:	The Presidency
Resubmission:	Every 5 years
Last modified:	09.03.2023

Introduction

Trier University of Applied Sciences sees itself as an internationally oriented university with regional roots. Information plays a central role in achieving its strategic goals and fulfilling its tasks in research, teaching and administration. Information forms the basis of almost all university-wide processes. The task of information security is to protect this information, whether in analogue or digital form, and the processes and systems required to process and store it. In this way, it makes a significant contribution to ensuring that Trier University of Applied Sciences can fulfil its legal mandate and its voluntary commitments.

Information security at Trier University of Applied Sciences is based on the German Data Protection Regulation (DSGVO) and the current guidelines on IT-Grundschutz published in the IT-Grundschutz-Kompendium[1] of the Federal Office for Information Security (BSI) and the IT -Grundschutz-Profil für Hochschulen[2] derived from it by ZKI e.V..

The Presidency of Trier University of Applied Sciences is committed to the objectives of information security and its responsible implementation. The guideline on information security documents this commitment and formulates the strategic and organisational framework of information security at Trier University of Applied Sciences.

Scope

The guideline applies to all persons and institutions that use the IT infrastructure, networks and connected IT systems of Trier University of Applied Sciences at any location of Trier University of Applied Sciences or operate IT systems themselves in this environment.

Goals

The information security measures are intended to ensure an appropriate level of security, based on a risk analysis, in order to prevent damage to Trier University of Applied Sciences. In order to achieve the desired level of security and to comply with the respective applicable legal and contractual regulations, the following goals are strived for:

Availability:

> Systems, applications and data must be available to authorised persons as intended and on time in every situation.

Confidentiality:

> Data of any kind may only be accessed and used by authorised persons in a defined and permissible manner.

Integrity:

> The integrity of data must be maintained at all times. This also includes that information and data cannot be created or changed without authorisation.

[1] BSI IT-Grundschutz-Kompendium (in the respective current version, last accessed on 01.03.2023)
[2] IT-Grundschutz-Profil für Hochschulen (last accessed on 01.03.2023)

Strategy

Information Security Management

To achieve the security goals, an information security management system (ISMS) is established, which defines organisational structures and processes that are continuously monitored, evaluated and adapted to current requirements. This requires seamless asset management and suitable methods of monitoring.

The ISMS forms the core of the security strategy and includes the following components in particular:

Raising awareness

The members of the university are enabled by appropriate measures to comprehend the significance of information security within the scope of their activities, to understand the necessity of measures and to align their own actions with the general security objectives.

Risk management

Operational risk management comprises the regular process of identifying risks, assessing and evaluating risks, handling risks, monitoring risks and communicating risks relating to information security. The risk analysis is used in consultation with the Executive Board to select and implement suitable measures to deal with or minimise these risks. These measures are documented in the information security concept, which is reviewed annually.

Special organisational measures are the information security guidelines to be published, which provide specifications on how to deal with certain risks. They are binding and are reviewed annually.

Incident management

Responsibilities and procedures are defined for handling security-relevant incidents. Emergency concepts and plans are designed to ensure the resumption or continuation of business operations even in emergency and crisis situations while maintaining information security. This also includes the definition of a crisis management team.

Stakeholders and their tasks

Presidency

The overall responsibility for information security lies with the Presidential Board of Trier University. It provides the necessary resources, adopts the present guideline on information security and arranges for its review after 5 years at the latest.

Information Security Officer (ISB)

The Presidency appoints an Information Security Officer (ISB) at Trier University of Applied Sciences, who is a qualified specialist responsible for the area of information security. The focus is on a university-wide, holistic perspective that includes administration, research and teaching. The appointed person for information security is only bound by instructions from the Presidency in matters of information security.

He or she is responsible for the conception, control, documentation and further development of the ISMS as well as for risk analysis, investigation of security incidents and reports to the Executive Board on the status of information security. The person in charge is responsible for creating the information security concept and the guidelines derived from it together with all those involved in the security process. The necessary resources and information are made available to fulfil these tasks.

In consultation with the Presidency, the person has the right to issue instructions on critical issues of information security.

If an information security team is established, several persons can be appointed as information security officers.

Senate Information Security Officer (SBIS)

The Senate Information Security Officer is appointed by the Senate. The tasks include the strategic further development of the ISMS, risk analysis and advice on information security issues in coordination with the ISB. The SBIS is a member of the Information Security Team.

Crisis Management Team

The crisis management team controls and coordinates all measures in the event of security incidents that affect information security. The core team consists of ISB, SBIS, DPO and the management of the central computer centres. If necessary, the team is supplemented by persons from the Presidential Board and, if necessary, persons from affected institutions.

Management of the central IT departments

The management of the central data centres is responsible for the security of the IT infrastructure and the centrally operated and supported IT systems and ensures the implementation of the security measures.

People responsible for IT systems

Responsibility for information security basically follows the responsibilities for IT systems, i.e. every person who operates an IT system in the network of Trier University of Applied Sciences is responsible for the proper and secure operation of the system over its entire lifetime until it is decommissioned and disposed of properly.

Data Protection Officer (DSB)

The Data Protection Officer assesses the information security measures with regard to data protection. He or she must be involved in security incidents involving personal or other sensitive data.

Rights and duties

Participation

Users of the IT infrastructure at Trier University of Applied Sciences handle large amounts of information on a daily basis. For the protection of this information to succeed, the cooperation of all these people is imperative. They protect information, processes and systems according to their value to the best of their knowledge and ability.

Communication

In the event of information security risks and incidents, the ISB and the immediate superior must always be informed immediately. Communication with third parties outside the university is always carried out by the ISB, the DPO or the Presidential Board.

The ISB shall be involved in a timely manner in the conception, introduction and redesign of information-processing systems and processes.

Emergency intervention

In case of imminent danger, the ISB and the persons directly responsible for the affected IT systems or processes are entitled to take immediately necessary defensive measures. The principle of proportionality of means must be observed in the measures to be taken. The measures should be taken in such a way that affected users - if at all possible - are informed in advance. Depending on the nature of the incident, all relevant bodies must be informed afterwards (Presidium, DPO, ISB, staff representatives).

Coming into force

This guideline on information security for Trier University of Applied Sciences shall enter into force upon its publication on 14.04.2023. It is valid until revoked. The General Staff Council approved it on 03.04.2023.

Glossary

BSI	Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de) Federal Office for Information Security
DPO	Data Protection Office
DSGVO	Datenschutz-Grundverordnung (dsgvo-gesetz.de) Basic Data Protection Regulation
ISB	Informationssicherheitsbeauftragte Information Security Officer
ISMS	Information Security Management System
SBIS	Senatsbeauftragter für Datenschutz und Informationssicherheit Senate Commissioner for Data Protection and Information Security
ZKI e.V.	Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (zki.de)