Hochschule Augsburg
University of Applied Sciences

Information Security Policy at

Augsburg University of

Applied Sciences

Preamble

Providing quality IT services is crucial to running a successful university. Users' trust in information technology forms the basis for positive outcomes. In order to earn their trust, IT services and data management must demonstrate integrity, confidentiality and accessibility.

To fulfil this responsibility, all departments and institutions at Augsburg University of Applied Sciences must commit to supporting information technology. This policy is meant to strengthen this effort and serve as the basis for on-going information security management.

This methodological approach puts in place necessary rules and appropriate measures which protect information and data in such a way that

(1) adequately ensures confidentiality and prevents access by unauthorised persons,
(2) demonstrates integrity through accuracy and completeness,
(3) facilitates availability so that authorised users can easily use the IT resources at any time,
(4) adheres to legal requirements (e.g. The Bavarian Data Protection Act).

§1 Policy Objectives

The policy defines the basic regulations concerning the following information security goals:

(1) Protect the network infrastructure and IT systems, including the data they process, against internal and external misuse or sabotage.
(2) Establish information security measures to ensure a robust, reliable and safe university environment for teaching, research and administration.
(3) Provide secure and trustworthy online services for users at the university and beyond.
(4) Comply fully with the data protection requirements as set forth by law.
(5) Prevent and minimise damage caused by security infractions.

§2 Scope

This policy broadly covers information technology as a whole and address all university members and other external users who use or provide IT services. All faculties and central facilities of Augsburg University of Applied Sciences must comply with them. External service providers working on Augsburg University of Applied Sciences IT systems must also adhere to them.

$3 Information Security Management

The information security management system takes into account all the organizational and technical measures necessary to achieve a certain degree of information security (security level) and maintain it in the long term. In order to obtain a sufficient security level, additional measures for information requiring increased protection are defined using risk analysis.

Security plans will detail the specific regulations necessary to establish a sufficient security level and explain how to implement the underlying principles. They give sufficient detail on the requirements of this policy.

The security measures necessary to ensure the protection of information assets in everyday work, within projects or for services offered can be derived from these security plans.

At a minimum, the security plans shall cover the following areas:

(1) Organization of IT security
(2) Determination of information assets (classification)
(3) Access control, network security and operational security
(4) IT systems (such as servers, storage systems, workstations)
(5) Detection of vulnerable areas and protection against malware
(6) Handling security incidents
(7) Backup and emergency planning
(8) Risk management, compliance and data protection
(9) Physical safety
(10) Communication

The central IT security officer is in charge of running the information security management system. They also advise the IT committee and IT representatives from the faculties as well as the computer centre.

By regularly reviewing the implementation of the security plan and further developing security measures, the officer helps secure a sufficient level of information security.

They have the authority to review IT security across the university.

IT services with remote access must be evaluated by the IT security officer as well as the data protection officer.

§4 Responsibility for IT security

The IT working group (IT Arbeitskreis) is in charge of the information security management system. The IT security officer acts on behalf of the IT working group and methodologically coordinates the information security management system.

The president's office has the final authority over assumption of risk and implementation measures as it is also responsible for properly maintaining university operations and information security.

In order to continuously develop the policy and related documents (e.g. the security plan), IT working group meetings regularly include information security as an item on their agenda. The IT security officer provides status reports and is assigned tasks based on decisions made by the IT working group.

The senate is to be consulted before information security policies are adopted.

All university employees, as individuals who own and process information, are responsible for maintaining the information security level in their unit.

§5 Classification of Information

All information assets must be classified according to the information classification plan set out in the security plan. The owner of the information performs this task. This classification is based on the value and sensitivity of the respective information assets and aims to achieve a sufficient security level.

§6 Access to Information and Data

Access to data and IT systems is controlled by technological means and processes that correlate to the value and importance of the data and systems.

Anyone who uses the applications/IT systems must be clearly identifiable and must have received the appropriate authorisation and authentication for their specific function and task.

Access is further limited based on the minimal rights principle, which means that authorisation is only granted to the extent necessary for the fulfilment of a given task.

Any final decisions or changes to important information must be properly logged and documented. Information owners determine the importance of the information and thus whether it is necessary to log and document such changes and how to do so.

§7 Security Awareness

In order to reach the required level of information security, employees must be made aware of information security threats. They must also know their individual areas of expertise and personal duties and conduct themselves responsibly.

Training sessions and information materials will be provided to university members to help familiarise themselves with security regulations and other relevant issues.

§8 Risk Intervention / Security Incidents

When the IT security of critical systems at the university is at risk, a service representative from the computer centre, together with the CIO, can immediately shut down the affected IT system and temporarily ban the users responsible for creating the threat. The handling of security incidents must follow the documented process in place for such IT security incidents. The IT working group decides which IT services require emergency plans, which the IT security officer then collects and coordinates. The emergency plans describe what to do in risk situations and system errors.

§9 Come into effect

These statutes come into force on the day after their publication.

Issued on the basis of the decision of the Senate of July 11, 2017 and the approval of the President of the Augsburg University of Applied Sciences of October 27, 2017.

Augsburg, October 27th, 2017

Prof. Dr. Gordon T. Rohrmair

President

This English version was translated from the German version that were laid down at the university on November 25, 2017; the resignation was announced on November 25, 2017 by a notice in the university.

The day of the announcement is November 25th, 2017.