UNIVERSITÄT MANNHEIM

Information Security Policy

of the University of Mannheim

Photo credit: Norbert Bach

Version 1.0 as at 2 April 2025
Document classification: “TLP white – public”

Contact: Department of Information Security
E-mail: infosicherheit@uni-mannheim.de

Document classification with TLP

This document is classified as "TLP white – public" with the Traffic Light Protocol (TLP). The classification is also indicated on the cover page, where it is highlighted in color according to the table below.

TLP indicates regulations for the disclosure of a document and thus increases security. The recipient of a document must comply with the classification on the cover page. A detailed explanation of the disclosure regulations can be found in the table below.

TLP classification	Disclosure regulations
TLP white - not limited	The document does not contain any confidential information and may be disclosed and made available to the public without any restrictions, except for copyright-related issues.
TLP green – restricted to university	This document contains information required for work purposes. It may be forwarded to partners of the university, but it must not be published.
TLP amber – confidential (…)	This document contain confidential information and may only be disclosed to a limited number of persons defined in advance (e.g., UNIT, University Library, Chair X). Disclosure to third parties is only possible if the third persons require the document for fulfilling their work duties and are aware of the TLP classification. Upon classification of the document, the group of persons defined in advance must be added in brackets.
TLP red – strictly confidential (…)	This document contains strictly confidential information that may only be disclosed to a limited number of persons defined in advance; mostly these are also participants in a meeting, conference, or written correspondence (e.g., President's Office). Disclosure is prohibited. Upon classification of the document, the group of persons defined in advance must be added in brackets.

Table of Contents

1 Preamble

The University of Mannheim has been educating students to become professionals in business, research, and society for generations and is one of the best research institutions in Europe. “Information” as a commodity plays a key role in research, teaching, and administration. This includes the knowledge of employees as well as paper-based knowledge and knowledge that is processed by information technologies (IT).

As university operations have become increasingly modern, the university has become highly dependent on functioning and secure IT. The university’s dependency is regularly challenged by a variety of vulnerabilities and threats[1]. In particular, cyberattacks are attempting to bring university operations to a halt. Information security ensures secure and uninterrupted operations.

With this Information Security Policy, the President’s Office of the University of Mannheim emphasizes the importance of information security and the corresponding information security management for the university.

Thus, this policy lays the foundation for information security management at the University of Mannheim.

2 Scope

This policy as well as the guidelines based on it apply to the entire University of Mannheim. It applies to all persons, including third parties, who process university-related information or use its information processing systems.

The Information Security Policy takes effect upon publication and, without delay, is to be observed by all employees.

From the date on which the Information Security Policy comes into force, third parties who are contracted by the University of Mannheim are obliged to comply with the requirements of this policy to the necessary and reasonable extent when new tenders and contracts are issued.

3 Goal of Information Security

A main goal of information security is to maintain the university’s capacity to act, i.e., to avoid disruptions in research, teaching, and administrative operations. The focus is to ensure the three security

[1] This includes, for instance: physical threats, human mistakes, technical errors and failures, social engineering, malware, inadequate security guidelines, or outdated software.

objectives of confidentiality[2], integrity[3], and availability[4] to an appropriate extent, even if absolute security cannot be guaranteed.

A violation of these security objectives, for example, in the form of disclosure of confidential information, manipulation of systems or information, or loss of data, causes a disruption of university operations.

4 Information Security Process

Information security is not an achievable condition. Extensive information security needs to be maintained and improved constantly as part of a continuous process. The University of Mannheim takes a risk-based approach.

The process focuses on the university's capacity to act. The strategic goals of information security are based on this capacity to act and are laid out in the Information Security Strategy of the University of Mannheim. Risk-based measures to protect the university are developed in line with the strategic goals. These measures are the basis for further action.

Taking into account available resources, they are then prioritized in a way that allows for the maximum security level to be achieved. Prioritization and measures are regularly reviewed in terms of effectiveness and updated if necessary.

5 Classification of this Information Security Policy

The following paragraphs describe and distinguish between the Information Security Policy, Information Security Strategy, and Information Security Guidelines. The Information Security Policy and the Information Security Strategy are valid at the same level. The Information Security Guidelines are secondary to the policy.

---

[2] "Confidentiality is the protection against unauthorized disclosure of information. Only authorized persons may access confidential data and information in a lawful way". (Federal Office for Information Security, IT-Grundschutz Compendium, second edition 2023).

[3] "Integrity means ensuring the correctness (intactness) of data and the correct functioning of systems. [...] Therefore, loss of integrity can mean that data are altered without permission, information on the author is altered, or the dates of creation are manipulated". Federal Office for Information Security, IT-Grundschutz Compendium, second edition 2023).

[4] "The availability of services, functions of an IT system, IT applications or IT networks, or the availability of information is given if these can be used as intended by the users" (Federal Office for Information Security, IT-Grundschutz Compendium, second edition 2023).

5.1 Information Security Policy

In line with the commitment of the President's Office to information security, this policy forms the basis for all further information security structures, processes, measures, and guidelines. For this purpose, it describes the persons involved in information security, their responsibilities, as well as the process chosen to facilitate information security at the University of Mannheim.

5.2 Information Security Strategy

The concrete information security goal is specified in the currently valid Information Security Strategy of the University of Mannheim. The Information Security Strategy defines the university's strategic goals regarding information security and the corresponding measures for their implementation. As a rule, the Information Security Strategy is revised every four years to ensure that both the current state of the art regarding technology as well as current risks and attack scenarios are considered when selecting measures to be implemented.

5.3 Information Security Guidelines

Information Security Guidelines describe requirements and instructions on a specific topic and for a defined target group. They are essential for implementing measures across all areas of the university and thus maintaining the university's capacity to act.

6 Roles and Responsibilities

In addition to universal responsibilities that apply to every person in the scope, there are particular roles with specific responsibilities. This section first describes the universal responsibilities and then the specific roles.

The President's Office bears the overall responsibility for information security and has established the steering committee for information security to manage it at the strategic level. Furthermore, the University of Mannheim operates the Department of Information Security headed by the Chief Information Security Officer (CISO). In its role as the main IT service provider, the University IT is in particular responsible for securing the university's IT, in particular the central IT infrastructure.

6.1 General Responsibilities

Effective protection of information requires everyone's cooperation. Every person who falls within the scope of this policy must, to the best of their knowledge and within the scope of their authority, ensure that information security is maintained and that necessary security measures are implemented. In particular, this obliges the University IT and all other operators of IT systems and their infrastructure to implement technical and organizational measures to protect these systems and infrastructure. If necessary, the Chief Information Security Officer supports the technical implementation on an organizational level or advises the responsible staff members. In addition, if necessary, they provide contacts to service providers or training material.

In order for the university to be able to track and control the implementation status of measures to increase information security, these measures must be documented and kept up to date by the respective controllers and institutions in an appropriate form.

In the event of vulnerabilities[5] and negative, security-relevant events[6] that potentially jeopardize the security of the university, its members, its systems or its data, it is of great importance to involve the CISO early in the process in order to ensure an adequate response. Such vulnerabilities and security-relevant events must therefore be reported immediately to the CISO.

When designing projects and permanent job profiles, time and budget for information security must be adequately taken into account. If necessary, the CISO can support the individual planning process.

6.2 Chief Information Security Officer

The Chief Information Security Officer (CISO) heads the Department of Information Security. They are responsible for the implementation of information security at the University of Mannheim within the framework set by this policy, the Information Security Strategy and the strategic decisions of the steering committee for information security, while also serving in an advisory capacity.

The CISO strategically plans and monitors organizational and technical measures and processes to ensure information security in order to establish information security at the university in the long term. Specific planning, implementation and continuous improvement are the responsibility of the CISO, the UNIT or other institutions or persons, depending on the measure and the process.

In particular, the CISO is responsible for the organizational aspects of information security. This includes steering the information security process, consulting tasks, planning and implementing awareness and training measures and handling information security incidents.

The CISO also draws up and updates the information security policy and the Information Security Strategy, which are then submitted to the President's Office as a draft for approval. They coordinate and support the establishment of university-wide Information Security Guidelines. The specific production of a guideline takes place in coordination with the CISO by the respective controllers and institutions. The CISO in coordination with the steering committee for information security submits the documents to the President's Office for approval.

At least once a year, the CISO reports directly to the President's Office about the current status of information security at the university.

Possible conflicts of interest must be avoided when selecting the CISO. In particular, the CISO may not take on any other roles that could lead to such conflicts. Among other things, this excludes the role of the Chief Information Officer (CIO) and the Head of the University IT.

---

[5] A weakness or flaw in an application, IT system, component, network infrastructure or process that can be exploited by attackers.

[6] Examples of negative events that need to be reported are: stolen laptops, computers infected with Trojans, compromised servers, responses to phishing emails and leaked data in general.

The CISO must be independent in order to adequately complete their role. This means that superiors are not allowed to influence evaluations of information security. In order to safeguard this independence, professional, disciplinary and financial aspects must be taken into account.

6.3 President's Office

The President's Office is responsible for information security at the University of Mannheim. It ensures that information security is implemented, maintained and further developed at the University of Mannheim in accordance with this policy.

The President's Office receives the CISO's reports. The status of information security at the University of Mannheim as described in this report is reviewed at least once a year by the President's Office to ensure that it is adequately fulfilling its responsibilities as laid out in this policy.

The information security policy and the Information Security Strategy are approved by the President's Office. University-wide Information Security Guidelines also require approval of the President's Office. The authority to approve a guideline can be delegated to other departments or roles.

The President's Office is responsible to provide resources to implement and maintain information security. Taking into consideration the entire range of tasks at the university, the President's Office provides the CISO and the University IT with resources in terms of finances and time, in order for them to be able to attend regular continuing education programs and information procurement as well as to realize the goals and measures described in the Information Security Strategy of the University of Mannheim to an economically feasible extent.

6.4 Steering Committee for Information Security

The steering committee is tasked with prioritizing existing measures and new measures not previously included of the Information Security Strategy, review their status and, if necessary, develop proposals for decisions for the President's Office. The preparation of the individual proposals for the President's Office is the responsibility of the institutions or persons responsible for the respective measure.

The members of the steering committee for information security are by virtue of their office:

- CISO (managing director),
- Executive Vice President,
- the Vice President who is responsible for information security
- CIO,
- Head of the University IT accompanied by the person responsible for operational IT security.

6.5 University IT

The University IT is responsible for the university's central IT infrastructure. It is their task is to create the necessary technical infrastructure and processes to protect information security and to implement the necessary technical measures. To this end, the University IT is in close contact with the CISO.

7 Cooperation

As all higher education institutions in the Land of Baden-Württemberg face similar challenges when it comes to establishing information security. The CISO is to regularly exchange information with the relevant stakeholders of Baden-Württemberg. This way, synergies can be exploited despite local differences between the higher education institutions. This is to be supported by bwInfoSec, the cooperation network for information security of the higher education institutions in Baden-Württemberg. As part of the cooperation network, the CISO is to take part in the cooperation between the CISOs and local staff members in information security and jointly develop suitable solutions. Moreover, the CISO is to continuously exchange information with other higher education institutions beyond the cooperation network and Baden-Württemberg.

8 Entry into Force

The information security policy applies to all employees from the day after its announcement. They must comply with it without delay, that is, as quickly as can be reasonably expected from their subjective point of view.