Information Security Guideline for the Technical University of Darmstadt

–Translation help, the German version is binding–

Information Security TU Darmstadt

Published: April 05, 2024

TECHNISCHE UNIVERSITÄT DARMSTADT

!nfoSec TU Darmstadt

Contents

Preamble

The operation of a university depends to a large extent on the quality of its IT services. Maintaining information security is therefore of fundamental importance. This means that the integrity, confidentiality and availability of IT processes, IT systems, IT services and all types of information and data must be protected in a sustainable manner.

In order to fulfill this obligation in the face of a growing threat situation and evolving technology, all university institutions must see the protection of information technology as a common challenge that is tackled in a continuous information security process on the basis of a uniform and binding information security strategy for the university. The basic prerequisite for success is an appropriate balance between the requirements of academic freedom and the fulfillment of relevant information security requirements.

§ 1 Subject of the guideline

This Information Security Guideline (ISLL) is the leading document regulating information security at the Technical University of Darmstadt (hereinafter referred to as "TUDa") and provides an overview of the applicable security structure with all necessary roles and responsibilities. This ISLL is used to formulate information security objectives and compliance with them in order to support the overall objectives of TUDa.

The implementation of TUDa's information security concept is based, among other things, on the following framework conditions, compliance with which is essential for the implementation of our own information security objectives:

- Information Security Guideline for the Hessian State Administration
- Hessian law for the protection of electronic administration (Hessisches IT -Sicherheitsgesetz - HITSiG)
- Hessisches E-Government-Gesetz (HEGovG)
- Security standards, in particular BSI Standards 200-1 to 200-4 and the BSI IT-Grundschutzkompendium
- EU-DSGVO, BDSG-neu, Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG), § 55 Hessisches Hochschulgesetz (HessHG)

§ 2 Area of application

The ISLL covers all TUDa business processes and the information and data processed therein, IT components operated by or for TUDa, the entire IT operation and all workstations located inside and outside the campuses managed by TUDa.

It is binding for the Presidential Board, all institutions, members and affiliates of the university as well as other actors and persons who are commissioned with information security-related activities for and on behalf of TUDa or who operate and / or use IT infrastructure within the TUDa information network for other reasons. The same applies to all partners of TUDa not mentioned in the above list whose actions affect the information security interests of TUDa.

§ 3 Objectives of information security

The overriding objectives are the implementation and maintenance of an appropriate level of information security, which result from legal and regulatory requirements and our own obligations to the members and affiliates of the university and its partners. This includes the protection of all information and data with regard to its confidentiality, integrity and availability. This also applies in particular to research and teaching and the protection of research data and results. In addition, TUDa has the following safety objectives:

- Compliance with the legal, contractual and regulatory requirements to which TUDa is subject
- Establishment of clear responsibilities for defined information security processes
- Creating and maintaining safety awareness among all persons in accordance with *§ 2 Area of application*
- Establishing an organizational structure for the implementation of information security processes
- Establishing a process for recognizing and handling security incidents and implementing appropriate emergency management
- Commitment to the continuous improvement of the existing information security organization and processes as well as the handling of deviations and exceptions

§ 4 Information security strategy

An information security management system (ISMS) is implemented in accordance with the BSI standards 200-1 to 200-4 (BSI Grundschutz) to ensure that TUDa fulfills its tasks and meets its business and security objectives. Security measures are implemented for all processes, procedures and the required IT components with regard to the identified need for protection in order to ensure confidentiality, integrity and availability. Possible security risks to the information values are identified, analyzed, evaluated and assessed with regard to necessary measures and implemented if necessary. All safety-relevant specification and verification documents are subject to a revision cycle.

As the highest management level, the Executive Board has overall responsibility for the implementation, further development and continuous improvement of the ISMS. For internal management, tasks are distributed across several roles and responsibilities as well as committees. Those responsible are obliged to undergo regular further training and to appoint a deputy. This is intended to ensure the continuous maintenance of information security processes and an appropriate level of security.

§ 5 Roles and responsibilities in the information security organization

Overall responsibility for the implementation of information security lies with the Executive Board. An organizational structure for the security organization at TUDa was defined by the Executive Board to achieve all information security goals. It is crucial for the success of information security measures that all roles and committees are provided with sufficient resources for their tasks. For each role, a representative must be appointed who can assume the tasks and

responsibilities in the event of a necessary substitution.

The following roles are involved in the information security process at TUDa and are shown in the 1 figure:

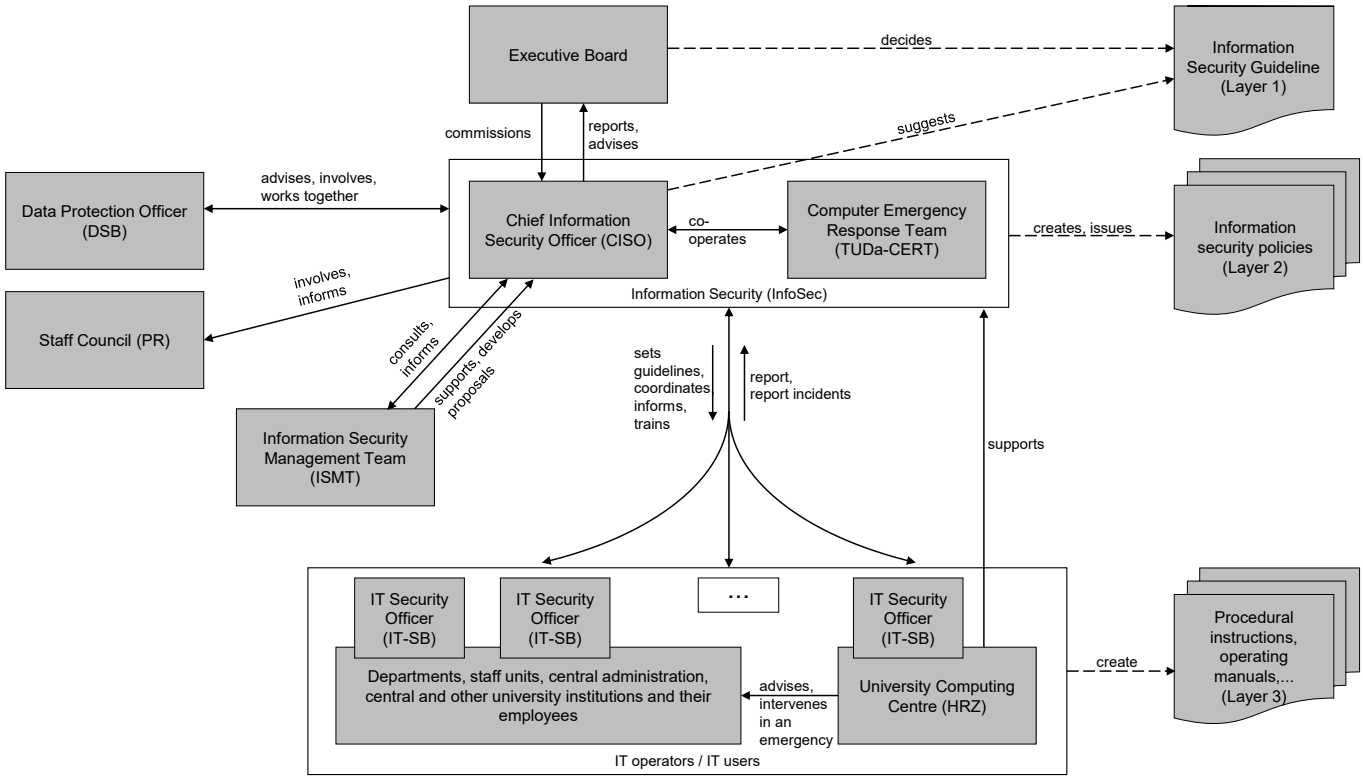

Figure 1: Roles and responsibilities in the information security organization. With regard to ISMS document structure, see also *§ 6 Regulatory structure for information security*.

(1) **Executive Board of the University**

The tasks of the Executive Board include deciding and managing the information security strategy and objectives as well as the digitalization strategy. The Executive Board may delegate tasks for the implementation of and compliance with these to subordinate responsibilities.
Information security lies within the purview of the responsible member of the Executive Board. In particular, he/she is responsible for the quality control and supervision of the information security organization.

The Executive Board and all managers actively exemplify the implementation of information security at TUDa and thus serve as a motivating role model for all employees. The Executive Board receives regular reports on the status of information security from the responsible Chief Information Security Officer and decides on necessary measures. Overall responsibility and possible risk assumption lie with the Executive Board.

(2) **Chief Information Security Officer (CISO)**

The CISO is appointed by the Executive Board and reports directly to the Executive Board. The CISO is the head of TUDa's central information security department (InfoSec), which is organizationally assigned to the responsible member of the Executive Board as a staff unit. She/he heads the IT Security Officers (IT-SB) and the Computer Emergency Response Team (TUDa-CERT, see (4)) and represents the interests of the Presidential Board towards all subordinate responsibilities and committees in the information security process.

The CISO is responsible for the establishment, operation and further development of the information security organisation at TUDa, draws up and issues overarching information security guidelines, advises the Executive Board as well as Data Protection and Business Continuity Management and coordinates the implementation of TUDa's overarching IT emergency and IT crisis management. He/she is the central contact person for all internal and external information security-related issues and is responsible for the university-wide information and communication system through which all those involved in the information security process are in contact.

The CISO regularly reports to the Executive Board on the current status of information security, coordinates the implementation and effectiveness of information security measures, awareness-raising and training measures and advises on internal and external projects relating to information security issues. In particular, he/she is responsible for writing and sending the annual IT security report to the Hessian state government and coordinates it with the responsible member of the Executive Board.

The Executive Board provides the necessary resources for the fulfillment of the function and implementation of necessary tasks and ensures regular further training for the CISO. The CISO has situational consultation, directive, and veto rights in all decisions concerning the area of responsibility for information security and must be involved in all pending initiatives (e.g., new projects or changes to the IT infrastructure).

The CISO is authorised to obtain all information relevant to the information security process [1] from the individual institutions and is authorised to issue instructions with regard to information security.

The CISO is independent and not subject to directives in his/her specialist areas.

The duties, rights and obligations apply analogously to the representative.

(3) **Information security management-Team (ISMT)**

An ISMT is formed due to the close interlinking of the topics and the overarching goals of TU Darmstadt. In accordance with BSI Standard 200-2, the ISMT supports the CISO by coordinating overarching measures in the overall organisation, collating information and carrying out control tasks.

The ISMT currently consists of

- one representative of the Executive Board (the responsible member of the Executive Board),
- the CISO,
- the TUDa-CERT management,
- a representative of the IT security officers and
- a representative of the management of the HRZ.

By resolution of the ISMT, it can be expanded to include additional persons if necessary (such as the university's data protection officer (DSB, see (8)), advisory experts (e.g. for operating systems such as Unix, Linux or Microsoft Windows), persons responsible for specific areas (e.g. for e-mail, network or user administration) or a representative of the staff council.

The members of the ISMT support the following tasks in their respective spheres of activity:

- Determine the information security objectives and strategies and further develop the information security guideline.

[1] If the collection takes place in the form of information protected by data protection law, this must be documented. If recurring processes arise in which personal data is regularly used, these processes must be described in a record of processing activities. Furthermore, the affected users must be notified in the cases prescribed by law. If data relating to the workplace and employment relationship of university employees is required, the Staff Council must be informed. If, for example in the context of an emergency, rapid action is required depending on the situation, this is sufficient afterwards.

- Review the implementation of the security guidelines.
- Initiate, control and monitor information security processes.
- To participate in the development of information security concepts.
- Check the effectiveness and suitability of the security measures planned in the security concepts.
- Design the awareness and training programmes for information security.

The ISMT is the central supervisory body for information security at TU Darmstadt and is headed by the representative of the Executive Board. The ISMT is responsible for implementing the ISLL, meets regularly and is tasked with drawing up proposals for the further development of information security regulations. The parties involved in the information security process can submit proposals to the ISMT.

(4) **Computer Emergency Response Team (TUDa-CERT)**

The TUDa-CERT is organisationally subordinate to the CISO and is part of InfoSec. The TUDa-CERT works confidentially and directly with the CISO, coordinates on key issues and reports to the CISO on its activities at regular intervals.

The TUDa-CERT consists of the management of the TUDa-CERT and other employees - information security experts, e.g. in the areas of: Network, identity management, e-mail server and gateway, critical infrastructure.

The tasks of TUDa-CERT are the overarching coordination and, at an operational level, the prompt response to information security incidents as well as misuse and improper utilisation of the information infrastructure. TUDa-CERT is responsible for designing and implementing measures to prevent security incidents and minimise any damage that may occur. The TUDa-CERT supports the CISO, the IT-SB and the ISMT in technical matters and intervenes independently to avert danger in the event of an IT emergency and coordinates the overarching countermeasures at an operational level. It regularly compiles a situation report on the IT security situation at TU Darmstadt for the ISMT. The management of TUDa-CERT reports regularly to the ISMT and the CISO on the operational measures. Furthermore, he/she reports immediately to the CISO in acute cases.

TUDa-CERT members are authorised to issue instructions to IT users and IT operators in IT emergencies and IT disruption and crisis situations. In particular, members of TUDa-CERT can order the immediate, temporary shutdown of the affected IT system and temporarily exclude the responsible users from using the information technology in the event of a breach of the applicable guidelines and to avert danger.

(5) **IT security officer(IT-SB)**

All areas, i.e. departments, staff units, central administration, central and other facilities of the university that operate IT systems, appoint an IT security officer. The responsibility can relate to several institutions and departments. The IT-SB is appointed exclusively from the university's full-time staff. If an institution does not appoint an IT-SB, the Executive Committee may appoint a temporary IT-SB. Until then, the management of the institution will fulfil these tasks. Further tasks and authorisations of the IT-SB are described in the subordinate ISMS documents (see *§ 6 Regulatory structure for information security*).

The roles are responsible for implementing the information security process in their institution. They are obliged to obtain up-to-date security-relevant information and are supported in this by the CISO. In addition, the system operators provide the IT-SB with all requested information that is necessary for reporting to internal and external superordinate bodies and make this available to the CISO in a complete and structured manner. The IT-SB shall initiate the necessary IT security measures in their area to avert danger. To this end, they must be given the necessary competences by the management of their institution. The provision of information must also be ensured towards TUDa-CERT.

(6) **The University Computer Centre (HRZ)**

The University Computer Centre (HRZ) plays a key role in ensuring information security and is responsible for IT emergency management for the services provided by the HRZ. HRZ employees support the CISO, the IT-SB, the TUDa-CERT and the ISMT in technical matters.

(7) **Departments, staff units, central administration, central and other university facilities and their employees**

Despite the appointment of the IT-SB, the responsibility of the heads of the departments, the staff units, the central administration, the central and other institutions as well as the affiliated institutions of the University for information security in their areas remains unaffected. They are obliged to involve the responsible IT-SB

and the CISO in all planning, procedures and decisions relating to information security. The users of the IT infrastructure assigned to them are bound by the regulations and specifications from the ISMS documents (see *§ 6 Regulatory structure for information security*), the TU Darmstadt user regulations and instructions from authorised information security roles.

(8) **Data protection officer of the university (DSB)**

The data protection officer assumes the tasks pursuant to Art. 39 GDPR. This responsibility ensures that all necessary measures for compliance with the HDSIG, BDSG-new and the EU GDPR are monitored. Furthermore, the CISO and the IT-SB are supported in ensuring the data protection of personal data in all IT-supported processes and procedures.

If data protection issues are involved in information security management, the university's data protection officer will be consulted.

The university's data protection officer shall review, upon written request from affected users, whether the collection of information was relevant and necessary for the information security process. The data protection officer informs the applicant, the ISMT and, if applicable, the Hessian Commissioner for Data Protection and Freedom of Information about the results of the review and can make recommendations for the future collection of information.

(9) **Staff Council of the University (PR)**

The University Staff Council is involved in accordance with § 69 of the Hessian Personalvertretungsgesetz. If workplace and personnel-related data of university employees is required as part of information security management, the Staff Council must be informed. If, for example in the context of an emergency, rapid action is required depending on the situation, this is sufficient afterwards.

The roles and responsibilities involved in the information security process work together constructively and in a solution-orientated manner in all matters relating to IT security. If necessary, external experts can be consulted for advice. The tasks and authorisations of the roles and responsibilities involved in the information security process are described in the subordinate ISMS documents (see *§ 6 Regulatory structure for information security*).

Information security incidents and emergencies of any kind must be reported. In the event of safety-relevant incidents, all parties involved are informed immediately, comprehensively and completely. The system operators are responsible for ensuring that the events are reported by the users themselves or by the system operators. If the report is made to the IT-SB, they must immediately forward the information to the TUDa-CERT and - if personal data is affected - to the official data protection officer.

§ 6 Regulatory structure for information security

(1) A hierarchical control structure has been established in TUDa for the implementation of all measures taken and the necessary documented information. These documents are subject to a regular revision cycle. Layer 1 comprises TUDa's information security guideline. It is approved by the Executive Board and reviewed at least every five years on its behalf.

(2) Layer 2 comprises detailed specifications in the form of guidelines that define binding framework conditions either for all or a specific group of people in accordance with*§ 2 Area of application*. Overarching requirements for the implementation of information security are documented in information security guidelines. The CISO is responsible for creating and maintaining the documents. Revision cycle: every 3 years or as required.

(3) Layer 3 comprises the concrete implementation of the specifications from layer 1 and layer 2. The documents at this layer regulate the implementation of specific information security requirements for individual areas and topics. These are generally procedural instructions, operating manuals or other similar documents. If additional documentation is required, additional guidelines, manuals or suchlike can be created. The system and process managers are responsible for creating, maintaining and communicating the information. Revision cycle: annually or as required.

In addition to the regulatory documents, there are additional verification documents, such as security concepts, reports, documentation, audit reports, protocols and similar. The system or process responsibles or process owners are

responsible for creating, maintaining and communicating the information. These documents are not part of the document pyramid and serve as extended documentation and as proof of the implementation of security measures of the information security management system.

Layer	Type of document	Level of detail and content
Layer 1	Guidelines	Binding requirements for all persons in accordance with *§ 2 Area of application*. Provides the strategic and organisational framework for information security management.
Layer 2	Information security guidelines	Mandatory requirements for all or a specific group of persons in accordance with *§ 2 Area of application*.
Layer 3	Procedural instructions, operating manuals, …	Binding specifications for specific/thematic areas, some of which are of a documentary nature.
	Handling aids, guidelines, safety concepts, …	Recommendations, configuration aids, detailed descriptions

Table 1: Document pyramid

§ 7 Continuous improvement

The ISMS must be reviewed regularly, at least annually, to ensure that it is up to date and effective. In order to maintain and further develop the system, effectiveness and success are regularly monitored and any non-conformities are rectified. This process serves to analyse the appropriateness, suitability and effectiveness of implemented measures and is supported by the Executive Board to increase efficiency and improve the level of information security.

This is implemented by means of internal audits, exercises, awareness-raising measures and technical vulnerability scans, among other things. Any deviations found are documented as part of the continuous improvement process and rectified within a reasonable timeframe using suitable measures or adjustments. The results of the effectiveness reviews are documented in a management report and reported to the Executive Board.

§ 8 Coming into effect

The ISLL comes into effect following the resolution of the Executive Board with its publication on the InfoSec website and on TUprints.