

 <p>Universität Hamburg DER FORSCHUNG DER LEHRE DER BILDUNG</p>	<p>Information Security Guideline for the University of Hamburg</p>	<p>IS-LL@UHH Version 1.2</p>
--	--	---

1 Objective

With the Information Security Guideline of the Free and Hanseatic City of Hamburg (IS-LL@FHH), the Senate has established generally binding principles for information security in the Hamburg administration. The IS-LL@FHH is the overarching guideline for the guidelines in the IT manual and serves the purpose of making all information in the Hamburg administration complete, correct, and available, while protecting it from unauthorized access. The Information Security Guideline of the University of Hamburg (IS-LL@UHH) specifies the IS-LL@FHH. An information security management system (ISMS-UHH) is to be established and operated within the university. The ISMS-UHH is based on the IT baseline protection catalogs of the Federal Office for Information Security.

2 Scope

The IS-LL@FHH applies to all departments of the Free and Hanseatic City of Hamburg (FHH), judicial authorities, and other public bodies of the FHH, insofar as they act on behalf of the state (due to state matters pursuant to §6 HmbHG, this also includes the UHH). The IS-LL@UHH applies to all institutions and bodies of the University of Hamburg.

3 Security concept

The University Information Security Management (InSiMa@UHH) develops a security concept that includes cross-faculty measures, framework guidelines for the presidential administration and the faculties, and guidelines for the central IT service provider (RRZ). This involves taking stock of information processes, determining protection requirements, deriving basic measures from these requirements, and specifying objectives.

With the participation of the RRZ, a university-wide, and if necessary, inter-university IT security incident response team (CERT Computer Emergency Response Team) will be set up at the RRZ using the DFN-CERT service already offered nationwide, and emergency and crisis management will be planned.

4 Responsibilities

All employees must ensure information security through responsible behavior and comply with the regulations relevant to information security (laws, ordinances, guidelines, staff representation agreements, organizational regulations, contractual obligations, etc.).

The UHH, represented by the president, establishes a university information security management system (InSiMa@UHH) by means of a decision by the executive committee and appoints an information security officer. The Executive Board or the Executive Board Administration shall enable employees to participate in training measures in the field of data security or, in consultation with the information security officer, shall inform them about information security issues in staff meetings or by other appropriate means.

Responsibility for information security in data processing on behalf of the UHH lies with the UHH in accordance with the HmbDSG.

5 University information security management

University information security management (InSiMa@UHH) consists of the management (information security officer as the person responsible for information security at the UHH as a staff unit, e.g. the president or the CIO) and the security team (approx. 5 employees from the areas of presidential administration, IT service providers such as RRZ, faculties, and data protection law such as 61). The main tasks include:

- Determining information security objectives and creating and updating the university's IS-LL,
- Developing and updating a university security concept,
- Checking whether the university IS-LL or the university security concept and the measures specified therein are being implemented and are effective,
- Interpreting the university IS-LL in cases of doubt,
- Implementing the cross-departmental and cross-faculty measures of the university security concept,
- Organization and implementation of training courses on information security,
- Investigation of incidents that compromise information security and determination of appropriate measures to prevent such incidents
- Advising the Executive Board and other UHH bodies on information security issues,
- Documenting the measures implemented and process changes in information security management.

InSiMa@UHH submits all regulations and measures to the Executive Board for consultation and decision-making. In the event of imminent danger or very urgent issues, InSiMa@UHH can implement appropriate measures directly. As recommended by the State Court of Auditors in the context of the IT orientation audit, the university information security officer participates in the regular meetings of the working group of official information security officers in order to jointly discuss information security issues and report to the Executive Board.

6 University Information Security Officer

The role of information security officer can be performed in addition to other tasks, but should not be performed by the IT management itself. The main tasks of the information security officer include:

- Advising university departments involved in information processes on information security issues
- Taking the lead in developing a university-wide security concept,
- Checking whether all prescribed information security measures are implemented and effective at the UHH,
- Participation in regular information exchange and in the working group of the central InSiMa,
- Reporting to the UHH bodies,
- Development of a training concept and instruction of employees in matters of information security,
- Preparation of an annual report on information security (as part of the Executive Board's annual report).

The Executive Board and the deaneries support the information security officer in the performance of his or her duties.

7 Entry into force

The IS-LL@UHH shall enter into force upon the information security officer taking up their duties.