1 Objective

With the information security guidelines of the Free and Hanseatic City of Hamburg (IS-LL@FHH), the Senate has defined generally binding principles for information security within the Hamburg administration. The IS-LL@FHH contains overarching principles for the guidelines laid out in the IT Handbook and serves to ensure that all information within the Hamburg administration is complete, correct, and available, and also protected from unauthorized access. Universität Hamburg's information security guidelines (IS-LL@UHH) supplement the IS-LL@FHH. An information security management system (ISMS-UHH) is to be set up and operated internally at the University that is based on the IT baseline protection (IT-Grundschutz) methodology 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), legal organs, and other public bodies of the FHH insofar as they act on behalf of the state. This includes Universität Hamburg due to state-commissioned matters pursuant to Section 6 of the Hamburg higher education act (Hamburgisches Hochschulgesetz, HmbHG). The IS-LL@UHH applies to all institutions and bodies at Universität Hamburg.

3 Security concept

The University's information security management team (InSiMa@UHH) prepares a security concept that includes cross-faculty measures, framework specifications for University Administration and the faculties, as well as specifications for the central IT service provider (RRZ). This involves reviewing the information processes, determining the protection needs, deriving fundamental measures from these, and setting goals.

The RRZ is involved in the setup of a University-wide (possibly cross-university) computer emergency response team (CERT) at the RRZ using the DFN-CERT service already offered nationally. An emergency and crisis management system is also planned.

4 Responsibilities

All employees must ensure information security by acting responsibly and complying with relevant regulations (laws, regulations, guidelines, staff representative agreements, organizational regulations, contractual obligations, etc.).

Universität Hamburg, represented by its president, establishes a university information security management team (InSiMa@UHH) and appoints an information security officer. The Executive University Board or University Administration offers employees training on data security or, in coordination with the information security officer, briefs them on security issues during staff meetings or via other appropriate channels.

In accordance with Hamburg's data protection and privacy act (Hamburgisches Datenschutzgesetz, HmbDSG), responsibility for information security when processing data on behalf of Universität Hamburg is in principle borne by Universität Hamburg.

5 University information security management team

The University information security management team (InSiMa@UHH) comprises one manager (information security officer as the person at Universität Hamburg responsible for information security, e.g., as an office of the Executive University Board or the chief information officer) and an information security team (approx. 5 employees from University Administration, IT service providers like the RRZ, and staff responsible for data protection regulations, e.g., Section 61). The team's main tasks are to:

- define information security goals and create and update the IS-LL@UHH;
- develop and maintain a university security concept;
- ensure that the IS-LL@UHH and the University's security concept and the measures specified therein are implemented and effective;
- interpret the university IS-LL in cases of doubt;
- implement the cross-departmental and cross-faculty measures laid out in the University's security concept;
- organize and implement training on information security;
- investigate incidents impacting information security and define appropriate measures to prevent these;
- advise the Executive University Board and other bodies at Universität Hamburg on information security matters;
- document the measures implemented and process changes in information security management.

InSiMa@UHH submits all regulations and measures to the Executive University Board for consideration and decision-making. In case of imminent threats and matters of utmost urgency, InSiMa@UHH can implement appropriate measures immediately. As recommended by the state court of auditors as part of the IT orientation audit, the University's information security officer attends the regular meetings of the working group of official information security officers in order to discuss information security issues and report back to the Executive Board.

6 Information security officer at Universität Hamburg

The job of the information security officer can be performed in addition to other tasks, though not by the IT management itself. The main tasks of the information security officer are to:

- advise the University departments involved in information processes on information security;
- supervise the development of a university-wide security concept;
- verify that all required information security measures are implemented and effective at Universität Hamburg;
- participate in the regular exchange of information and the working group of the central InSiMa;
- report back to the various bodies at Universität Hamburg;
- conceive training and brief employees on information security matters;
- prepare an annual report on information security (as part of the annual report of the Executive University Board).

The Executive University Board and the offices of the dean support the information security officer in the performance of her/his duties.

7 Effective date

The IS-LL@UHH becomes effective when the information security officer takes up her/his duties.