1 Zielsetzung

Mit der Informationssicherheitsleitlinie der Freien und Hansestadt Hamburg (IS-LL@FHH) hat der Senat allgemeinverbindliche Grundsätze für die Informationssicherheit in der Hamburgischen Verwaltung festgelegt. Die IS-LL@FHH ist übergeordnete Leitlinie für die Richtlinien des IT-Handbuches und dient dem Ziel, alle Informationen in der Hamburgischen Verwaltung vollständig, korrekt und verfügbar zu machen, aber sie vor unbefugtem Zugriff zu schützen. Die Informationssicherheitsleitlinie der Universität Hamburg (IS-LL@UHH) konkretisiert die IS-LL@FHH. Inneruniversitär soll ein Informationssicherheitsmanagementsystem (ISMS-UHH) aufgebaut und betrieben werden. Das ISMS-UHH orientiert sich dabei an den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik.

2 Geltungsbereich

Die IS-LL@FHH gilt für alle Dienststellen der Freien und Hansestadt Hamburg (FHH), Organe der Rechtspflege sowie die sonstigen öffentlichen Stellen der FHH, soweit diese im staatlichen Auftrag tätig werden (wg. staatlicher Auftragsangelegenheiten gem. §6 HmbHG auch die UHH). Die IS-LL@UHH gilt für alle Einrichtungen und Organe der Universität Hamburg.

3 Sicherheitskonzept

Das universitäre Informationssicherheitsmanagement (InSiMa@UHH) erstellt ein Sicherheitskonzept, das fakultätenübergreifende Maßnahmen, Rahmenvorgaben für die Präsidialverwaltung und die Fakultäten als auch Vorgaben für den zentralen IT-Dienstleister (RRZ) umfasst. Dazu erfolgen eine Bestandsaufnahme der Informationsprozesse, die Feststellung der Schutzbedarfe, die daraus abzuleitenden grundsätzlichen Maßnahmen und die Konkretisierung der Ziele.

Unter Mitwirkung des RRZ wird ein universitätsweites, ggf. hochschulübergreifendes IT-Sicherheitsvorfallteam (CERT Computer Emergency Response Team) unter Nutzung des bereits bundesweit angebotenen DFN-CERT-Dienstes beim RRZ eingerichtet sowie ein Notfall- und Krisenmanagement geplant.

4 Zuständigkeiten

Alle Beschäftigten haben die Informationssicherheit durch ihr verantwortliches Handeln zu gewährleisten und die für die Informationssicherheit relevanten Regelwerke (Gesetze, Verordnungen, Richtlinien, personalvertretungsrechtliche Vereinbarungen, organisatorische Regelungen, vertragliche Verpflichtungen u. ä.) einzuhalten.

Die UHH, vertreten durch den Präsidenten, richtet über einen Präsidiumsbeschluss ein universitäres Informationssicherheitsmanagement (InSiMa@UHH) ein und benennt eine/n Informationssicherheitsbeauftragte/n. Das Präsidium bzw. die Präsidialverwaltung ermöglicht den Beschäftigten Schulungsmaßnahmen auf dem Gebiet der Datensicherheit bzw. setzt sie in Abstimmung mit der/dem Informationssicherheitsbeauftragten in Dienstbesprechungen oder auf andere geeignete Weise über die Belange der Informationssicherheit in Kenntnis.

Die Verantwortung für die Informationssicherheit bei Datenverarbeitung im Auftrag der UHH trägt grundsätzlich die UHH gemäß HmbDSG.

5 Universitäres Informationssicherheitsmanagement

Das universitäre Informationssicherheitsmanagement (InSiMa@UHH) besteht aus der Leitung (Informationssicherheitsbeauftragte/r als Verantwortliche oder Verantwortlicher für Informationssicherheit in der UHH als Stabsstelle z.B. des/der Präsidentin/en bzw. des/der CIO) und dem Sicherheitsteam (ca. 5 Beschäftigte aus den Bereichen Präsidialverwaltung, IT-Dienstleister wie z.B. RRZ, Fakultäten und Datenschutzrecht wie z.B. 61). Zu den wesentlichen Aufgaben gehören:

- Bestimmung der Informationssicherheitsziele und Erstellung sowie Fortschreibung der universitären IS-LL,
- Entwicklung und Fortschreibung eines universitären Sicherheitskonzepts,
- Prüfung, ob die universitäre IS-LL bzw. das universitäre Sicherheitskonzept und die darin vorgegebenen Maßnahmen umgesetzt werden und wirksam sind,
- Auslegung der universitären IS-LL in Zweifelsfällen,
- Umsetzung der abteilungs- und fakultätsübergreifenden Maßnahmen des universitären Sicherheitskonzepts,
- Organisation und Durchführung von Schulungen zur Informationssicherheit,
- Untersuchung von Vorfällen, die die Informationssicherheit beeinträchtigen, und Festlegung geeigneter Maßnahmen zur Vermeidung solcher Vorfälle,
- Beratung des Präsidiums und anderer Organe der UHH in Informationssicherheitsfragen,
- Dokumentation der durchgeführten Maßnahmen und Prozessveränderungen im Informationssicherheitsmanagement.

Das InSiMa@UHH legt alle Regelungen und Maßnahmen dem Präsidium zur Beratung und Beschlussfassung vor. Bei Gefahr im Verzuge oder sehr dringlichen Themen kann das InSiMa@UHH entsprechende Maßnahmen direkt in Kraft setzen. Wie vom Landesrechnungshof im Rahmen der IT-Orientierungsprüfung empfohlen, nimmt der/die universitäre Informationssicherheitsbeauftragte an den regelmäßigen Sitzungen der Arbeitsgruppe der behördlichen Informationssicherheitssbeauftragten teil, um Themen zur Informationssicherheit gemeinsam zu beraten und dem Präsidium zu berichten.

6 Universitäre/r Informationssicherheitsbeauftragte/r

Die Funktion der/des Informationssicherheitsbeauftragten kann zusätzlich zu anderen Aufgaben, sollte aber nicht von der IT-Leitung selbst wahrgenommen werden. Zu den wesentlichen Aufgaben der/des Informationssicherheitsbeauftragten gehören:

- Beratung der mit Informationsprozessen befassten Stellen der Universität in Fragen der Informationssicherheit,
- Federführung bei der Erstellung eines universitätsweiten Sicherheitskonzepts,
- Prüfung, ob in der UHH alle vorgeschriebenen Maßnahmen zur Informationssicherheit umgesetzt werden und wirksam sind,
- Teilnahme am regelmäßigen Informationsaustausch bzw. an der Arbeitsgruppe des zentralen InSiMa,
- Bericht an die Organe der UHH,
- Erstellung eines Schulungskonzeptes und Unterrichtung der Beschäftigten in Fragen der Informationssicherheit,
- Erstellung eines jährlichen Berichtes zur Informationssicherheit (als Teil des Jahresberichtes des Präsidiums).

Das Präsidium und die Dekanate unterstützen die/den Informationssicherheitsbeauftragte/n bei der Wahrnehmung ihrer/seiner Aufgaben.

7 Inkrafttreten

Die IS-LL@UHH tritt mit dem Dienstantritt der/des Informationssicherheitsbeauftragten in Kraft.