Informationssicherheitsleitlinie

DER HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG

Inhalt

1. Präambel

Die HAW Hamburg stellt die exzellente Qualität von Studium und Lehre innerhalb einer forschenden Hochschule in den Mittelpunkt. Nur so können nachhaltige Lösungen für die vielfältigen Herausforderungen heute und in Zukunft entwickelt werden. In diesem Sinne profitieren wir von unserer Vielfalt und sehen diese als Stärke.

Die Informations- und Kommunikationstechnik (IKT) ist dabei von zentraler Bedeutung für die Erfüllung unserer Aufgaben in Forschung und Lehre. Die Digitalisierung entlang der in der Digitalisierungsstrategie und dem SEP der HAW Hamburg definierten Ziele, schreitet weiter voran und stellt nicht nur wichtige Prozesse und Werkzeuge zur Verfügung, sondern ermöglicht es , unsere Qualität in dem Bereichen Studium und Lehre sowie in Forschung und Verwaltung stetig zu verbessern und die Vernetzung mit unseren vielfältigen Kooperationspartnern voranzutreiben.

Nur durch die Bereitstellung einer verlässlichen und vertrauenswürdigen Infrastruktur können wir den Betrieb in allen Bereichen der HAW Hamburg erfüllen und sicherstellen. Hierbei handelt es sich um eine Querschnittsaufgabe, da nicht alle Sicherheitsmaßnahmen zentral erbracht werden können. Hierfür spricht auch der dezentrale und eigenständige Charakter unserer Einrichtungen mit vielen eigenständig erbrachten Abläufen und Prozessen mit der dezentralen Speicherung und Verarbeitung von Informationen auf dezentral betriebener IKT. Der Schutz der verarbeiteten Informationen und die Sicherheit der eingesetzten IKT – Infrastruktur und Systeme – ist somit eine grundlegende Voraussetzung für ein angemessenes Sicherheitsniveau in der gesamten HAW Hamburg. Dieses einheitlich und übergreifend zu erreichen kann nur durch das Zusammenwirken zentraler – und hier hat das ITSC eine herausgehobene Verantwortung – und dezentraler Einrichtungen erfüllt werden. Dies zu erreichen ist damit die gemeinsame Aufgabe aller Einrichtungen der Hochschule, aller Verantwortlichen und aller Nutzer*innen der IKT-Infrastruktur und IKT-Systeme.

Insbesondere die aktuellen Erfahrungen in der Praxis zeigen immer wieder, dass trotz umfangreicher vorbeugender Maßnahmen, Schwachstellen bei den technischen und organisatorischen Maßnahmen nicht auszuschließen sind. Auch die HAW Hamburg muss daher mit Sicherheitsvorfällen umgehen und hierauf vorbereitet sein, um die Folgeschäden zu minimieren und betroffene Funktionen schnell wieder sicher anbieten oder nutzen zu können. Dazu gehört auch, dass die Verantwortlichen über die verbleibenden Restrisiken informiert sind und die Kontrolle über die Verarbeitungsprozesse aktiv wahrnehmen und verantworten können. Wichtig ist, dass Informationssicherheit und Datenschutz zusammenwirken müssen, denn ohne eine wirksame Informationssicherheit kann der Datenschutz nicht gewährleistet werden.

Ziel ist es insgesamt, Missbrauch und Risiken einzudämmen, die die Vertraulichkeit der verarbeiteten Informationen, deren Integrität und Verfügbarkeit gefährden könnten. Ebenso muss die Authentizität der Prozesse, Systeme und Nutzer*innen und die Ordnungsmäßigkeit der Verarbeitungsprozesse sichergestellt werden. Hierfür muss auch eine generelle Verfügbarkeit der IKT-Infrastruktur und die Anbindung an das deutsche Wissenschaftsnetz als Übergang ins globale Internet robust gewährleistet sein.

Es müssen eine Vielzahl unterschiedlicher Aspekte berücksichtigt werden: neben den technischen und infrastrukturellen Rahmenbedingungen sowie den verschiedenen organisatorischen Regelungen und Vorgaben, sind die sehr unterschiedlichen Interessen sowohl der Einrichtungen der HAW Hamburg als auch der Nutzer*innen abzuwiegen. Dies führt im Einzelfall zu Einschränkungen bzgl. der Verfügbarkeit von Funktionen, der Bedienbarkeit oder des Komforts, wenn andernfalls die Anforderungen an Informationssicherheit oder Datenschutz nicht erfüllt werden können. Die erzielten Kompromisse müssen von allen Nutzer*innen der HAW Hamburg akzeptiert und mitgetragen werden.

2. Geltungsbereich

Diese Leitlinie gilt für alle angegliederten, sowie eigenständigen Einrichtungen und Organe, die zur HAW Hamburg gehören, IKT der HAW Hamburg einsetzen oder die für Informationsverarbeitung aufgebaute IKT-Infrastruktur nutzen bzw. in diese integriert sind.

Gleichzeitig bezieht sie sich auf Informationen inklusive personenbezogener Daten sowohl in digitaler als auch analoger Form sowie auf die technischen Systeme, mit denen solche Informationen verarbeitet werden. Auch analoge (z.B. Ausdrucke, Aufzeichnungen) als auch digitale (z.B. Festplatten, Wechseldatenträger, Cloud-Speicher) Medien, die schützenswerte Informationen enthalten, fallen in den Geltungsbereich.

3. Detaillierte Ziele der Informationssicherheit

Mit der Informationssicherheitsleitlinie für die Freie und Hansestadt Hamburg (IS-LL, Version 1.0 vom 2. April 2013) hat der Senat allgemeinverbindliche Grundsätze für die Informationssicherheit in der Hamburgischen Verwaltung festgelegt. In dieser Hinsicht ordnet sich die Informationssicherheitsleitlinie der HAW Hamburg der IS-LL unter, soweit es die Verwaltung der HAW Hamburg selbst betrifft. In Hinblick auf die Einrichtungen der Forschung und Lehre, die nicht der Verwaltung zuzuordnen sind, werden die Anforderungen und Forderungen sinngemäß und mit dem Ziel eines angemessenen Sicherheitsniveaus für die gesamte Hochschule angewandt. Hier muss insbesondere verhindert werden, dass von einzelnen Bereichen mit niedrigeren Sicherheitsanforderungen (z.B. Labore für die Lehre) eine Gefährdung für Bereiche mit höheren Sicherheitsanforderungen (z.B. die Verwaltung) ausgeht.

Die in der Präambel bereits grundlegend angesprochenen Ziele müssen weiter detailliert werden, da diese den Ausgangspunkt für alle weiteren Richtlinien und Konzepte darstellen. Gleichzeitig dienen die hierdurch definierten Anforderungen als Maßstab für die Analyse und Bewertung von Risiken der Informationsverarbeitung sowie des Einsatzes von IKT-Systemen und -Infrastrukturen insgesamt.

Die im weiteren erläuterten Ziele sind gleichrangig zu verstehen, da es zunächst gilt, alle Anforderungen zu erfassen. Hierzu gehören auch alle vertraglichen und gesetzlichen Anforderungen, die unabhängig von unserer eigenen Bewertung oder Einschätzung bei der

Informationsverarbeitung gelten. Außerdem gelten diese Ziele unabhängig davon, ob es sich um Informationen der HAW Hamburg selbst handelt, oder uns diese von Kooperationspartnern anvertraut wurden.

- **Vertraulichkeit –** Schutz vor unberechtigten Zugriffen auf Informationen incl. dem Schutz bei der Übertragung über unsichere Kommunikationsnetze
- **Besitz und Kontrolle –** Schutz vor Verlust der Kontrolle bei der Übertragung von Informationen in den Verantwortungsbereich Dritter incl. der Speicherung in Cloud-Infrastrukturen oder -Plattformen
- **Integrität –** Schutz vor unberechtigten Veränderungen von Informationen, IKT-Systemen und/oder -Infrastrukturen
- **Authentizität –** Schutz vor unberechtigten Zugriffen auf Anwendungssysteme und IKT-Systeme oder -Infrastrukturen oder dem Vortäuschen falscher Identitäten im Rahmen des Identity Managements der HAW Hamburg
- **Verfügbarkeit –** Schutz der Verfügbarkeit von IKT-Systemen und -Infrastrukturen incl. der Anbindung an das Wissenschaftsnetz sowie der Anwendungssysteme und Informationen
- **Verbindlichkeit –** Schutz vor Manipulation von Transaktionen oder dem Vortäuschen falscher Transaktionen bei der Nutzung oder Verarbeitung von Informationen oder der Verwendung von Anwendungssystemen
- **Compliance –** Einhaltung der geltenden Vorgaben und rechtlichen Bestimmungen incl. der Wahrung der Persönlichkeitsrechte der Nutzer*innen und des Rechts auf informationelle Selbstbestimmung

4. Prinzipien für den Informationssicherheitsprozess

Da die Informationssicherheit einen hohen Stellenwert hat und zwingend für einen adäquaten Datenschutz notwendig ist, muss diese als integraler Bestandteil der Organisation und aller Geschäftsprozesse (Querschnittsaufgabe) angesehen und verantwortet werden. Um die damit verbundenen Ziele erreichen zu können, müssen verschiedene Aufgaben wahrgenommen und kontrolliert werden. Hierzu wird eine Informationssicherheitsbeauftragt*e (InSiBe) benannt und ein Informationssicherheitsmanagementsystem (ISMS) etabliert, welches stetig und messbar verbessert wird.

Folgende Prinzipien liegen allen Entscheidungen und getroffenen Maßnahmen zur Informationssicherheit im Geltungsbereich dieser Leitlinie zugrunde:

- zentrale und dezentrale IKT-Systeme werden in einer dem identifizierten Schutzbedarf entsprechenden, sicheren Umgebung betrieben
- zentrale und dezentrale IKT-Systeme werden bei Schwachstellen gemäß des identifizierten Schutzbedarfs und Risikos zeitnah auf einen sicheren Versionsstand gebracht
- zentrale und dezentrale IKT-Systeme werden durch kompetentes Personal nachhaltig und verantwortungsvoll betreut
- die administrative Arbeit auf zentralen und dezentralen IKT-Systemen wird sicher und nachvollziehbar gestaltet
- Daten und Informationen werden vor unberechtigten Zugriffen geschützt und entsprechend des identifizierten Schutzbedarfs angemessen und sicher verarbeitet

- erkannte Sicherheitsvorfälle werden bearbeitet und dokumentiert mit dem Ziel, Ursachen sowie Schwachstellen zu identifizieren, um diese zu beheben und das ISMS stetig zu verbessern
- die Wiederherstellung von Informationen und IKT-Systemen und -Infrastrukturen erfolgt innerhalb der durch den identifizierten Schutzbedarf definierten Zeiträume, um die Funktionsfähigkeit der Hochschule zu gewährleisten
- wenn durch Umweltfaktoren, Angriffe oder Vorfälle die Funktionsfähigkeit der Hochschule in wesentlichen Teilen über längere Zeit eingeschränkt wird, muss dies im Rahmen eines dem ISMS übergeordneten Krisenmanagements adressiert werden
- durch eine begleitende Revision der Regelungen und der Überprüfung der IKT-Systeme und -Infrastrukturen wird das angestrebte Informationssicherheitsniveau sichergestellt
- identifizierte Abweichungen werden mit dem Ziel analysiert, das Sicherheitsniveau zu verbessern und ständig auf dem aktuellen Stand der Technik zu halten sowie die Compliance des Betriebs sicherzustellen
- die Verantwortlichkeit für Informationssicherheit folgt grundsätzlich den Zuständigkeiten für Informationen, IKT-Systeme und IKT-Infrastrukturen
- Alle Nutzer*innen haben ein Grundverständnis für Belange der Informationssicherheit und insbesondere des Datenschutzes
- Alle Nutzer*innen haben die Pflicht und Verantwortung, Ereignisse, die die Informationssicherheit im Sinne dieser Leitlinie beeinträchtigen könnten, schnellstmöglich dem ITSC zur Kenntnis zu bringen
- Alle Nutzer*innen werden zu einer zweckmäßigen, verantwortungsvollen und ökonomischen Nutzung der IKT-Systeme und IKT-Infrastruktur angehalten
- Alle Nutzer*innen müssen in Hinblick auf die Bedeutung von Risiken der Informationssicherheit sowie insbesondere des Datenschutzes und der Anwendung allgemeiner und spezieller Schutzmaßnahmen geschult und sensibilisiert werden
- Alle Maßnahmen zur Informationssicherheit müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IKT-Systeme bzw. -Infrastrukturen stehen

Der InSiBe hat die Aufgabe, die Informationssicherheitsleitlinie und die Wirksamkeit der bisherigen Organisationsform, getroffener Maßnahmen und des Informationssicherheits-managementprozesses insgesamt weiterzuentwickeln und jährlich darüber zu berichten.

5. Organisation des Informationssicherheitsmanagement

Informationssicherheit ist nur in einem kontinuierlichen Prozess zu gewährleisten. In diesem wird auf der Basis offener und adäquater Kommunikation der verschiedenen beteiligten Personen und Rollen untereinander dafür Sorge getragen, dass Bedrohungen und damit verbundene Risiken identifiziert werden, um diese bewerten zu können und dann zu entscheiden, welche organisatorischen bzw. technischen Maßnahmen getroffen werden müssen. Hierbei können die Maßnahmen auf die Verringerung eines möglichen Schadens oder die Reduzierung der Eintrittswahrscheinlichkeit ausgerichtet sein.

Die Organisationsverantwortung für die Informationssicherheit liegt beim **Präsidium der HAW Hamburg**, vertreten durch den Präsidenten der HAW Hamburg. Der IT-Beirat bestehend aus Vertretern aller Fakultäten, der Hochschulverwaltung, des ITSC und der Vizepräsidentin für

Digitalisierung übernimmt die Funktion eines **Chief Information Officer (CIO)** -Gremiums, das die Hochschule in ihrer Gesamtheit betreffend ihrer Koordinierungsaufgaben im Bereich der Informationssicherheit, vertritt. Hierbei wird der IT-Beirat von dem Informations-sicherheitsbeauftragten (InSiBe) unterstützt.

Der von dem Präsidium ernannte **Informationssicherheitsbeauftragte** hat gemäß der Informationssicherheitsleitlinie (LL-IS) der FHH folgende wesentliche Aufgaben:

- Beratung der mit Informationsprozessen befassten Stellen der Behörde (z. B. Leitung Organisation, IT-Beauftragte oder IT-Beauftragter, IT-Leitungen) in Fragen der Informationssicherheit,
- Erstellung eines Sicherheitskonzepts, das die Rahmenvorgaben des zentralen Sicherheitskonzepts erfüllt und alle weiteren erforderlichen Maßnahmen zur Informationssicherheit in der jeweiligen Behörde beschreibt,
- Prüfung, ob in der Behörde alle vorgeschriebenen Maßnahmen zur Informationssicherheit umgesetzt werden und wirksam sind,
- Teilnahme am regelmäßigen Informationsaustausch bzw. an der Arbeitsgruppe des zentralen lnSiMa der FHH (Informationssicherheitsmanagement), und der Arbeitsgruppen der InSiBe der Hamburger Hochschulen,
- Unterrichtung der Beschäftigten in Fragen der Informationssicherheit.

Der InSiBe ist bzgl. seiner ihm übertragenen Aufgaben nur an Weisungen des Präsidiums gebunden. Das Präsidium stellt sicher, dass der InSiBe für seine Aufgaben in erforderlichem Umfang von seinen übrigen Aufgaben entlastet wird und sorgt für eine angemessene Ausstattung.

Der InSiBe hat ein Informations- und Vorschlagsrecht. Der InSiBe nimmt im angemessenen Umfang an Hochschulgremien teil, hat aber auch ein aktives Informationsrecht, sofern es die Themen der IKT-Systeme bzw. -Infrastruktur und der Informationssicherheit sowie des Datenschutzes betrifft. Das Vorschlagsrecht dient dazu, konkrete Bedarfe und Maßnahmen an die Verantwortlichen weiter zu melden bzw. auf offene Probleme oder Schwachstellen hinzuweisen.

Im Sinne einer höheren Wirtschaftlichkeit und Nachhaltigkeit sind bei allen Projekten, Beschaffungen oder Ausschreibungen für die IKT-Systeme und -Infrastrukturen die Aspekte der Informationssicherheit von Anfang an zu berücksichtigen und ggf. zeitnah mit Beteiligung des InSiBe den Schutzbedarf abzustimmen, bevor höhere Folgekosten entstehen.

Des Weiteren gehört auch die Koordinierung und Analyse bei kritischen Informationssicherheitsvorfällen oder neuen Bedrohungen von IKT-Systemen bzw. -Infrastrukturen zu den wichtigen Aufgaben des InSiBe.

Durch die Anbindung an das deutsche Wissenschaftsnetz des DFN-Vereins sind wir an das DFN-CERT (hochschulübergreifende Unterstützung bei Angriffen und Sicherheitsvorfällen) angebunden und nutzen dessen Dienste:

- **DFN-CERT Advisories** – Auswertung der tagesaktuellen Alarme und Meldungen zu neuen Sicherheitslücken und akuten Bedrohungen

- **DFN-CERT AutoWarn** – Hinweise auf konkrete Angriffe oder Angriffsversuche aus den angeschlossenen Netzen
- **DFN-CERT NeMo** – Überwachung und Alarmierung bei aktuellen verteilten Verfügbarkeitsangriffen (DDoS = Distributed Denial of Service)

6. Ausblick

Diese Informationssicherheitsleitlinie wird zukünftig durch weitere themenspezifische Richtlinien unterstützt bzw. detailliert werden, die die weitere Umsetzung von Maßnahmen innerhalb des Informationssicherheitsmanagements unterstützen und koordinieren. Hierzu gehören insbesondere:

- **Behandlung von Vorfällen**
- **Sicherheitschecks und Prüfprozesse**
- **Feststellung des Schutzbedarfs**

Um den notwendigen Schutz der Informationen und eingesetzten IKT-Systeme und -Infrastrukturen zu erreichen, werden technische und organisatorische Maßnahmen ergriffen, die dem identifizierten Schutzbedarf der Informationen bzw. Systeme oder Infrastrukturen angemessen sind. Die getroffenen Maßnahmen können hierbei dezentral verantwortet werden (z.B. Verschlüsselung von Laptops), zentral angeboten werden (z.B. Identity Management der HAW Hamburg) oder zusammen erbracht werden (z.B. Netzsegmentierung zur Trennung unterschiedlicher Sicherheitsbereiche). Hierfür werden nach Bedarf einzelne Sicherheitskonzepte erstellt, die die gewählten Maßnahmen festlegen und darstellen.

7. Inkrafttreten

Die Informationssicherheitsleitlinie der HAW Hamburg tritt mit Präsidiumsbeschluss vom 09.12.2021 in Kraft.