Informationssicherheitsleitlinie der Frankfurt University of Applied Sciences

Verabschiedet vom Präsidium am 22.10.2024

Präambel

Diese Leitlinie beschreibt, für welche Zwecke und mit welchen Strukturen Informationssicherheit innerhalb der Frankfurt University of Applied Sciences (Frankfurt UAS) hergestellt werden soll und konkretisiert dahingehend die Informationssicherheitsleitlinie für die Hessische Landesverwaltung. Sie beinhaltet die von der Frankfurt UAS angestrebten Organisationsstrukturen, Aufgabenzuordnungen und die verfolgte Sicherheitsstrategie. Sie bildet damit das Fundament für die Sicherheitsstandards an der Hochschule und sowohl die daraus abgeleiteten Sicherheitsrichtlinien und Prozesse als auch technische und organisatorische Maßnahmen.

1. Ziele

Hauptziel dieser Leitlinie ist der Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der an der Frankfurt UAS vorhandenen Informationen unter Berücksichtigung regulatorischer, datenschutzrechtlicher und sonstiger gesetzlicher Vorgaben.

2. Geltungsbereich

Diese Leitlinie erstreckt sich auf alle Einrichtungen der Hochschule (Fachbereiche, wissenschaftliche Einrichtungen, zentrale Einrichtungen und Sonstige), auf die gesamte informationsverarbeitende (IT-) Infrastruktur der Frankfurt UAS, einschließlich der darin betriebenen IT-Systeme sowie der Gesamtheit der Benutzenden. Eingeschlossen sind auch An-Institute und Einrichtungen außerhalb der Hochschule, die direkt an das Hochschulnetz angeschlossen oder die Mitnutzende des Internetanschlusses der Frankfurt UAS sind. Sie ist für alle Mitglieder der Hochschule und Nutzende der IT-Infrastruktur verbindlich.

3. Organisationsstruktur und Verantwortlichkeiten

3.1. Verantwortlichkeiten

Die Bedeutung, die Informationen zukommt und der einrichtungsübergreifende Charakter des Informationssicherheitsprozesses erfordern, dass die Gesamtverantwortung für den umfassenden Komplex der Informationssicherheit im Kompetenz- und Verantwortungsbereich des Präsidiums liegt.

Die Leitungen der Fachbereiche, der Dezernate, der Stabsstellen, der sonstigen Einrichtungen sowie der angeschlossenen Einrichtungen der Hochschule sind für die Informationssicherheit in ihrem jeweiligen Bereich verantwortlich.

Alle IT-Systeme und Prozesse, die an der Frankfurt UAS betrieben werden, stellen sogenannte Verfahren dar.

Verfahrensbetreibende sind diejenigen, die von der bzw. dem Auftraggebenden eines

Verfahrens zur Einführung des Verfahrens beauftragt wurden. Sie sind für die Koordination des gesamten Aufbauprozesses, den Betrieb und die Dokumentation verantwortlich. Verfahrensbetreibende und die jeweils Zuständigen für Daten, Informationen, Verfahren sowie für unterstützende Systeme sind verpflichtet, die Sicherheit der von ihnen betriebenen Systeme unter Beachtung aller Vorgaben wie z. B. Sicherheitsrichtlinien zu gewährleisten und bei einer Änderung ihre Verfahren und Verfahrensbeschreibungen schnellstmöglich anzupassen.

Alle Hochschulmitglieder und -angehörigen und sonstige Nutzende sind dafür verantwortlich, dass die Informationssicherheitsprozesse eingehalten und die festgelegten Sicherheitsmaßnahmen in ihrem Bereich umgesetzt werden. Unterstützt durch sensibilisierende Schulungen und Betreuung soll jede bzw. jeder im Rahmen ihrer bzw. seiner Möglichkeiten Sicherheitsvorfälle vermeiden. Sicherheitsrelevante Ereignisse sind den zuständigen Stellen umgehend zu melden, damit schnellstmöglich entsprechende Reaktionen eingeleitet werden können.

3.2. Gesamtorganisation, Beauftragte und Gremien

Am Informationssicherheitsprozess der Hochschule sind folgende Gremien und Funktionsträger*innen verantwortlich beteiligt:

- Das Präsidium,
- die bzw. der Informationssicherheitsbeauftragte,
- das Informationssicherheitsmanagement-Team (ISMT),
- die Stabsstelle Informationssicherheit,
- das Dezernat Digitalisierung,
- die weiteren Dezernate, die weiteren Stabsstellen, die sonstigen Einrichtungen sowie die angeschlossenen Einrichtungen der Hochschule,
- die Fachbereiche.

Das Präsidium setzt eine bzw. einen Informationssicherheitsbeauftragte*n und eine bzw. einen stellvertretende*n Informationssicherheitsbeauftragte*n ein. Das Präsidium setzt außerdem ein Informationssicherheitsmanagement-Team (ISMT) ein. Ständige Mitglieder des ISMT sind:

- der bzw. die Vizepräsident*in für Digitalisierung,
- die bzw. der Informationssicherheitsbeauftragte,
- die bzw. der Leitende der Stabsstelle Informationssicherheit,
- die bzw. der Leitende des Dezernats Digitalisierung.

3.3. Aufgaben der bzw. des Informationssicherheitsbeauftragten

Die bzw. der Informationssicherheitsbeauftragte ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution. In Ausübung der Funktion ist sie bzw. er weisungsungebunden. Die bzw. der Informationssicherheitsbeauftragte ist

unmittelbar dem Präsidium zugeordnet. Zuständiges Präsidiumsmitglied ist der bzw. die Vizepräsident*in für Digitalisierung. Die Aufgaben der bzw. des Informationssicherheitsbeauftragten ergeben sich aus der Informationssicherheitsleitlinie für die hessische Landesverwaltung. Hierzu gehören auch

- das Informationssicherheitsmanagementsystem (ISMS) aufzubauen, weiterzuentwickeln, zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
- die kontinuierliche Überprüfung des ISMS sowie der damit verbundenen Verfahrensbeschreibungen,
- das Präsidium hinsichtlich der Informationssicherheit zu beraten,
- die Erstellung der Sicherheitsrichtlinien, der Notfall- und Betriebskontinuitätsmanagementrichtlinien und anderer Dokumente zur Informationssicherheit zu koordinieren,
- die Realisierung von Sicherheitsmaßnahmen zu initiieren, beratend zu begleiten und zu überprüfen,
- dem Präsidium und dem ISMT über den Status der Informationssicherheit zu berichten,
- bei der Auswahl von Sicherheitslösungen zu beraten,
- Sicherheitsvorfälle zu untersuchen und aufzulösen,
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu konzeptionieren und koordinieren,
- Stellungnahme zu neuen oder veränderten Verfahrensbeschreibungen abzugeben.

3.4. Aufgaben des ISMT

Das ISMT koordiniert übergreifende Maßnahmen in der Hochschule, trägt Informationen zusammen und führt Kontrollaufgaben durch. Aufgaben des ISMT sind insbesondere:

- Informationssicherheitsziele zu bestimmen,
- zu überprüfen, ob die auf Basis der Sicherheitsrichtlinien festgelegten technischen und organisatorischen Maßnahmen wie beabsichtigt geeignet und wirksam sind, neue Sicherheitsrichtlinien zu erlassen und zu aktualisieren,
- die Umsetzung der Sicherheitsrichtlinien zu überprüfen,
- gemeldete Sicherheitsvorfälle zu bündeln, klassifizieren und geeignete Maßnahmen einzuleiten,
- die Schulungs- und Sensibilisierungsprogramme für Informationssicherheit zu initiieren.

Das ISMT tagt in einem regelmäßigen Turnus in protokollierten Sitzungen. Wichtige Entscheidungen des ISMT, insbesondere auch der Erlass oder die Aktualisierung von Sicherheitsrichtlinien, sind durch die bzw. den Informationssicherheitsbeauftragte*n in geeigneter Weise der Hochschulöffentlichkeit bekannt zu machen. Im Falle eines kritischen Sicherheitsvorfalls ist das ISMT umgehend zu informieren.

3.5. Aufgaben der Stabsstelle Informationssicherheit

Die Stabsstelle Informationssicherheit steht allen Hochschulmitgliedern und -angehörigen bei Fragen zur Informations- und IT-Sicherheit zur Verfügung. Sie ist zuständig für die operative Steuerung, Koordinierung und Umsetzung des ISMS und

- unterstützt die bzw. den Informationssicherheitsbeauftragte*n bei der Wahrnehmung ihrer bzw. seiner Aufgaben,
- unterstützt bei der Erstellung und Weiterentwicklung des ISMS, insbesondere der Sicherheitsrichtlinien
- begleitet bei der Erstellung von Verfahrensbeschreibungen,
- betreibt ein Meldesystem für Sicherheitsvorfälle,
- erfasst und initiiert die Auflösung von Sicherheitsvorfällen,
- führt Awareness- und Schulungsmaßnahmen zur Informationssicherheit durch.

4. Der Informationssicherheitsprozess an der Frankfurt UAS

4.1. Vorgehensweise

Die Hochschule orientiert ihren Informationssicherheitsprozess an den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten Grundsätzen und Bausteinen auf Basis von ISO 27001 und etabliert damit ein ISMS.

Der Informationssicherheitsprozess ist hochschulweit einheitlich und wird zentral gesteuert.

4.2. Dokumente

4.2.1. Informationssicherheitsleitlinie

Die Informationssicherheitsleitlinie definiert den strategischen und organisatorischen Rahmen des Informationssicherheitsmanagements. Sie wird vom Präsidium verabschiedet.

4.2.2. Informationssicherheitsrichtlinien

Informationssicherheitsrichtlinien legen auf taktischer Ebene konkrete Anforderungen an die Informationssicherheit fest. Sie werden von der bzw. dem Informationssicherheitsbeauftragten entwickelt und vom ISMT verabschiedet.

4.2.3. Verfahrensbeschreibungen

Die Verfahrensbeschreibungen beinhalten das Informationssicherheitskonzept für das jeweilige Verfahren. Es konkretisiert die Informationssicherheitsrichtlinien und das ISMS der Hochschule auf operativer Ebene. Die Verfahrensbetreibenden dokumentieren dort, welche technischen und organisatorischen Maßnahmen gemäß der Informationssicherheitsrichtlinien ergriffen wurden, um die Einhaltung der Informationssicherheitsrichtlinien sicherzustellen. Die Verfahrensbetreibenden sind für die Umsetzung der in der Verfahrensbeschreibung genannten Maßnahmen verantwortlich.

Die oder der Informationssicherheitsbeauftrage nimmt zu den Verfahrensbeschreibungen Stellung. Sie werden von den Verfahrensbetreibenden entwickelt und vom Präsidium freigegeben.

Verfahrensbeschreibungen dienen nicht nur der Informationssicherheit, sondern insbesondere auch der Genüge datenschutzrechtlicher und anderer Vorschriften, die nicht Gegenstand dieser Leitlinie sind.

5. Gefahrenintervention

Bei Verdacht auf einen schweren Sicherheitsvorfall können Mitglieder des Präsidiums, die bzw. der Leitende des Dezernats Digitalisierung, die bzw. der Informationssicherheitsbeauftragte und technisch Verantwortliche in ihren jeweiligen Bereichen die sofortige, vorübergehende Stilllegung betroffener IT-Systeme und/oder Netzwerkanschlüsse veranlassen, um Schaden von der Hochschule abzuwenden. Die Verfahrensbetreibenden und das ISMT sind unverzüglich zu informieren.

6. Inkrafttreten

Diese Leitlinie tritt nach ihrer Verabschiedung am Tag nach ihrer Bekanntmachung in Kraft. Sie ersetzt die IT-Sicherheitsleitlinie in der Fassung vom 09.02.2009.