Leitlinie

zur

Informationssicherheit

an der OTH Amberg-Weiden

1 Präambel

Der Betrieb einer Hochschule hängt in hohem Maße von der Qualität seiner IT-Dienstleistungen ab. Das Vertrauen der Benutzer in die Informationstechnik bildet die Grundlage für ihren erfolgreichen Einsatz. Um dieses Vertrauen zu rechtfertigen, muss die Integrität, Vertraulichkeit und Verfügbarkeit der IT-Dienste und Daten sichergestellt sein.

Die Begriffe IT- und Informationssicherheit werden an der OTH Amberg-Weiden synonym verwendet, da sowohl organisatorische als auch technische Sicherheitsmaßnahmen zum Schutz der Informationen geregelt werden.

Damit die Hochschulleitung ihrer Verantwortung angesichts einer wachsenden Bedrohung der sich rasch weiterentwickelnden Technik bei gleichzeitig begrenzter personeller und finanzieller Ausstattung der Hochschulen nachkommen kann, müssen sämtliche Einrichtungen der OTH Amberg-Weiden den Schutz der Informationstechnik als gemeinsame Herausforderung begreifen und die Hochschulleitung in der Bewältigung der Aufgaben unterstützen. Diese Aufgaben sollen auf der Basis dieser Leitlinie in einem kontinuierlichen Informationssicherheitsmanagement bewältigt werden.

Dieses methodische Vorgehen basiert auf notwendigen Regeln und verlangt Maßnahmen, um Informationen (und Daten) in einer Art und Weise zu schützen, dass

(1) ihre Vertraulichkeit in angemessener Weise gewahrt ist und die Kenntnisnahme nur durch berechtigte Personen erfolgen kann,
(2) ihre Integrität durch ihre Richtigkeit und Vollständigkeit sichergestellt ist,
(3) ihre Verfügbarkeit gewährleistet ist, damit sie von den autorisierten Benutzern zum gewünschten Zeitpunkt in Anspruch genommen werden können,
(4) ihre Authentizität jederzeit nachgeprüft werden kann und
(5) gesetzliche Verpflichtungen, wie beispielsweise die Datenschutzgrundverordnung (DSGVO), erfüllt werden können.

Zu diesem Zwecke ist ein zweckmäßiger Ausgleich zwischen akademischer Freiheit und Informationssicherheit erforderlich.

2 Gegenstand der Leitlinie

Dieses Dokument drückt die Ausrichtung und Verantwortung der OTH Amberg-Weiden aus und definiert Grundsatzregelungen für folgende Informationssicherheitsziele:

(1) Schutz der Netzwerkinfrastruktur und der IT-Systeme einschließlich der damit verarbeiteten Informationen gegen Missbrauch oder Sabotage von innen und außen.
(2) Sicherstellung eines robusten, verlässlichen und sicheren Lehr-, Forschungs- und Verwaltungsbetriebs.
(3) Realisierung sicherer und vertrauenswürdiger Online-Dienstleistungen für Nutzer/-innen in und außerhalb der Hochschule.
(4) Gewährleistung der Erfüllung der aus den gesetzlichen Vorgaben resultierenden Anforderungen an den Datenschutz.
(5) Schäden durch Sicherheitsvorfälle soll vorbeugend begegnet bzw. die Auswirkung derartiger Vorfälle minimiert werden.

3 Geltungsbereich

Diese Leitlinie erstreckt sich auf die gesamte Informationstechnik und sämtliche Anwender/-innen, die diese benutzen oder bereitstellen und ist damit verbindlich für alle Fakultäten, wissenschaftlichen und zentralen oder sonstigen Einrichtungen der Hochschule.

Sie ist für alle Anwender/-innen und Dienstleister/-innen der an der OTH Amberg-Weiden eingesetzten Informationstechnologien verpflichtend einzuhalten.

4 Informationssicherheitsmanagement

Das Informationssicherheitsmanagementsystem (ISMS) umfasst alle erforderlichen organisatorischen und technischen Maßnahmen, um einen definierten Grad an Informationssicherheit (Mindestniveau) zu erreichen und langfristig zu erhalten. Um ein adäquates Sicherheitsniveau zu erreichen, werden für Informationen, die höheren Schutzbedarf erfordern, zusätzliche Maßnahmen auf Basis einer Risikoanalyse definiert.

Der/die zentrale Informationssicherheitsbeauftragte ist für den reibungslosen Ablauf des Informationssicherheitsmanagementsystems verantwortlich. Er/sie berät die Hochschulleitung und den Informationssicherheitsrat bei der Entscheidung und unterstützt das Rechenzentrum sowie ggf. die Workgroup-Manager der Fakultäten/Abteilungen/Bereiche bei der Auswahl und Umsetzung von IT-Sicherheitsmaßnahmen. Der Informationssicherheitsrat, bestehend aus der Hochschulleitung und dem Chief Information Officer (CIO), steuert fachlich die Aufgaben und Prioritäten der/des Informationssicherheitsbeauftragten und bildet für die Hochschule das Kontrollorgan in Sachen Informationssicherheit.

Die notwendigen Sicherheitsziele, Grundsätze, spezifische Regeln und Prinzipien sind in einem Sicherheitskonzept erfasst. Dort findet eine ausreichende Detaillierung der Anforderungen dieser Leitlinie und des Sicherheitsniveaus in Form von Sicherheitsrichtlinien statt. Diese sind dann Basis für die notwendigen Sicherheitsmaßnahmen. Diese Maßnahmen sind in Umsetzungsanforderungen bzw. dienstspezifischen Sicherheitskonzepten dokumentiert.

Die Sicherheitsrichtlinien umfassen mindestens folgende Themen:

- Organisation der Sicherheit
- Zugriffssteuerung
- Informationsklassifizierung (und deren Handhabung)
- physische und umgebungsbezogene Sicherheit
- RZ-Betriebsabläufe, Systemänderungen
- Benutzerrichtlinie/-ordnung/-regelung und Telearbeit
- Datensicherung und Notfallmanagement
- Schutz vor Schadsoftware und Handhabung technischer Schwachstellen
- Schlüsselverwaltung und kryptographische Maßnahmen
- Trennung und Nutzung von Netzen und Netzdiensten
- Umgang mit Sicherheitsvorfällen
- Information, Schulung und Verbesserung
- Compliance und Datenschutz
- Lieferantenbeziehungen bzw. Outsourcing

Der/die Informationssicherheitsbeauftragte berichtet dem Informationssicherheitsrat und wird von diesem gesteuert. Mit regelmäßigen Prüfungen der Umsetzung des Sicherheitskonzepts und Weiterentwicklung der Maßnahmen sorgt er/sie für adäquate Informationssicherheit.

Im Auftrag des Informationssicherheitsrats darf er/sie sich Überblick über die Informationssicherheit in allen Bereichen der Hochschule verschaffen.

Dienste, die außerhalb der Hochschule, z. B. über das Internet, erreichbar sind, bedürfen der Prüfung und/oder Genehmigung durch den/die IT-Sicherheits- und Datenschutzbeauftragte(n).

5 Informationssicherheitsverantwortung

Die Lenkungsverantwortung für das Informationssicherheitsmanagementsystem liegt beim Informationssicherheitsrat. Der/die Informationssicherheitsbeauftragte handelt in dessen Auftrag, er/sie koordiniert und steuert methodisch den Ablauf des Informationssicherheitsmanagementsystems.

Die letztgültige Entscheidung liegt bei der Hochschulleitung in ihrer Gesamtverantwortung für den ordnungsgemäßen Betrieb und der Informationssicherheit der Hochschule.

Zur kontinuierlichen Weiterentwicklung der Leitlinie und abhängiger Dokumente ist Informationssicherheit ein fester Bestandteil der Agenda der regelmäßigen Treffen des Informationssicherheitsrats. Der/die Informationssicherheitsbeauftragte berichtet dem anwesenden Steuerungsgremium über den aktuellen Stand und erhält seine/ihre Aufgaben basierend auf den Entscheidungen des Informationssicherheitsrats (Delegation der Aufgaben zur IT-Sicherheit).

Jede(r) Beschäftigte und Studierende der Hochschule ist in seinem Wirkungsbereich für die Einhaltung des Informationssicherheitsniveaus verantwortlich.

Ausnahmeregelungen im Bereich der Forschung und Lehre sind mit einer Risikobewertung zu begründen und zu dokumentieren.

6 Informationsklassifikation

Jede Art von Informationen muss klassifiziert werden. Die Klassifikation der Daten erfolgt entsprechend ihres Stellenwertes und ihrer Sensibilität zur Entwicklung eines angemessenen Sicherheitsniveaus.

7 Zugriff auf Informationen und Daten

Der Zugriff auf Daten und Systeme wird durch technische Maßnahmen und Prozesse ausreichend, dem Wert und der Bedeutung der Daten oder Systeme entsprechend, gesteuert.

Alle Benutzer von Applikationen/Systemen sind eindeutig identifizierbar und werden entsprechend ihrer Funktion und Aufgabe autorisiert und authentisiert.

Es wird das Prinzip der minimalen Rechte angewendet, d. h. Berechtigungen werden nur in dem Umfang gewährt, wie dies zur Erfüllung der jeweiligen Aufgaben erforderlich ist.

Alle Veränderungen wichtiger Informationen und getroffene Entscheidungen müssen durch angemessene Protokollierung und Dokumentation nachvollziehbar sein.

8 Sicherheitsbewusstsein

Das geforderte Maß an Informationssicherheit kann nur erreicht werden, wenn die Hochschulangehörigen auf Bedrohungen der Informationssicherheit sensibilisiert sind, die eigenen Kompetenzen und Pflichten kennen und sich verantwortungsbewusst verhalten.

Sicherheitsrelevante Themen und Regeln werden den Hochschulangehörigen durch geeignete Schulungs- oder Informationskanäle zur Kenntnis gebracht.

9 Gefahrenintervention und Sicherheitsvorfälle

Bei Gefahr der Verletzung der IT-Sicherheit kritischer Systeme der Hochschule können ein(e) Service-Verantwortliche(r) des Rechenzentrums gemeinsam mit einem Mitglied des Informationssicherheitsrats, die sofortige, vorübergehende Stilllegung des betroffenen IT-Systems anordnen, sowie die verantwortlichen Benutzer/-innen vorübergehend von der Nutzung der Informationstechnik ausschließen.

Der Informationssicherheitsrat bestimmt die IT-Dienste, für die der/die zentrale Informationssicherheits-beauftragte/Notfallkoordinator/-in des Rechenzentrums Notfallpläne sammelt und koordiniert. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen und unterteilen sich in einen allgemein zugänglichen Benachrichtigungsplan und in ein detailliertes Notfallkonzept für den Dienstgebrauch.

Der Umgang mit Sicherheitsvorfällen erfolgt entsprechend einem dokumentierten Prozess zur Behandlung von IT-Sicherheitsvorfällen. Dieser enthält alle notwendigen Maßnahmen, Verantwortlichkeiten, Berichtswege und Eskalationsschritte, die vor, während bzw. nach einem derartigen Vorfall maßgeblich sind.

10 Finanzierung

Die Hochschule muss den Beteiligten am Informationssicherheitsmanagementsystem ausreichend Mittel zur Verfügung stellen, damit diese ihre Aufgaben unverzüglich, umfassend und vollständig erfüllen können.

11 Inkrafttreten

Diese Richtlinie tritt am Tage nach ihrer Bekanntmachung in Kraft.

Amberg, den 17.12.2019

Prof. Dr. Andrea Klug Präsidentin

Dokumenteninformationen

Klassifikation:	V1 (öffentlich)
Titel:	Leitlinie zur Informationssicherheit
Versionsnummer:	1.2
Stand vom:	02.05.2025
Compliance-Bezug	
Dokumentenverantwortlicher:	Barbara Kostial (ISB)
Freigabedatum:	17.12.2019
Freigabe durch:	Präsident/in
Mitgeltende Dokumente:	Basisdokument unterschrieben von Prof. Dr. Andrea Klug in der Dokumentversion 1.0 vom 17.12.2019 (Inkrafttreten)
Revisionsintervall:	3 Jahre
Letzte Revision:	02.05.2023

Dokumentenverteiler

Verteilerkreis (Berechtigte Rolle):	Jeder

Dokumentenhistorie

Datum	Bearbeiter	Version	Bemerkung/Änderung
09.12.2019	Prof. Dr. Andreas Aßmuth, CIO	1.0	Erstellung
02.05.2023	Barbara Kostial (ISB)	1.1	Review; Layoutanpassung
02.05.2025	Barbara Kostial (ISB)	1.2	Review; Logo-Änderung; Änderung V2 zu V1 aufgrund Audit 2025

(Das Dokument basiert auf einer Vorlage, die von Herrn Christian Fötinger von der Stabsstelle Informationssicherheit bayerischer Hochschulen und Universitäten erstellt und zur Verfügung gestellt wurde.)