Hochschule Augsburg
University of Applied Sciences

Leitlinie

zur Informationssicherheit

an der Hochschule Augsburg

Präambel

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

Damit die Hochschule dieser Verantwortung nachkommen kann, müssen sämtliche Einrichtungen den Schutz der Informationstechnik unterstützen. Diese Aufgaben sollen auf der Basis dieser Leitlinie in einem kontinuierlichen Informationssicherheitsmanagement bewältigt werden.

Dieses methodische Vorgehen basiert auf notwendigen Regeln und verlangt angemessene 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 Personen zum gewünschten Zeitpunkt in Anspruch genommen werden können,
(4) gesetzliche Verpflichtungen (z.B. Bayerisches Datenschutzgesetz) erfüllt werden können.

§1 Gegenstand der Leitlinie

Dieses Dokument definiert Grundsatzregelungen für folgende Informationssicherheits-ziele:

(1) Schutz der Netzwerkinfrastruktur und der IT-Systeme einschließlich der damit verarbeiteten Daten gegen Missbrauch oder Sabotage von innen und außen.
(2) Sicherstellung der Informationssicherheit für einen robusten, verlässlichen und sicheren Lehr-, Forschungs- und Verwaltungsbetrieb.
(3) Realisierung sicherer und vertrauenswürdiger Online-Dienstleistungen für NutzerInnen 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 Vorfälle minimiert werden.

§2 Geltungsbereich

Diese Leitlinie erstreckt sich auf die gesamte Informationstechnik und sämtliche Hochschulmitglieder und externe AnwenderInnen, die diese benutzen oder bereitstellen. Sie ist verbindlich für alle Fakultäten und zentralen Einrichtungen der Hochschule. Sie ist auch von externen Dienstleistern der an der Hochschule Augsburg eingesetzten Informationstechnologien verpflichtend einzuhalten.

§3 Informationssicherheitsmanagement

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

Die notwendigen und spezifischen Regeln zur Erreichung des adäquaten Sicherheitsniveaus und Umsetzung der Prinzipien sind in einem Sicherheitskonzept erfasst. Dort findet eine ausreichende Detaillierung der Anforderungen dieser Leitlinie und des erforderlichen 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 Bereiche:

(1) Organisation der IT-Sicherheit
(2) Bestimmung der Informationswerte (Klassifikation)
(3) Zugriffssteuerung, Netzwerk- und Betriebssicherheit
(4) IT-Systeme (wie Server, Speichersysteme, Arbeitsplatzrechner)
(5) Erkennung von Schwachstellen und Schutz vor Schadsoftware
(6) Umgang mit Sicherheitsvorfällen
(7) Backup und Notfallplanung
(8) Risikomanagement, Compliance und Datenschutz
(9) Physische Sicherheit
(10) Kommunikation

Der/die zentrale IT-Sicherheitsbeauftragte ist für den Ablauf des Informationssicherheitsmanagementsystems verantwortlich. Er/Sie berät den IT-Ausschuss und die IT-Beauftragten der Fakultäten sowie das Rechenzentrum.

Mit regelmäßigen Prüfungen der Umsetzung des Sicherheitskonzepts und Weiterentwicklung der Maßnahmen sorgt er/sie für adäquate Informationssicherheit.

Er/Sie darf sich Überblick über die IT-Sicherheit in allen Bereichen der Hochschule verschaffen.

Von der Hochschule angebotene Dienste, die von außerhalb des Hochschulnetzes erreichbar sind, bedürfen der Prüfung durch den/die IT-Sicherheits- sowie den/die Datenschutzbeauftragten.

§4 Informationssicherheitsverantwortung

Die Lenkungsverantwortung für das Informationssicherheitsmanagementsystem liegt beim IT-Ausschuss. Der/Die IT-Sicherheitsbeauftragte handelt im Auftrag des IT-Ausschusses und koordiniert methodisch das Informationssicherheitsmanagementsystem.

Die letztgültige Entscheidung über Risikoakzeptanz und Umsetzungsgrad liegt beim Präsidium in dessen Gesamtverantwortung für den ordnungsgemäßen Betrieb und der Informationssicherheit der Hochschule.

Zur kontinuierlichen Weiterentwicklung der Leitlinie und abhängiger Dokumente (z.B. Sicherheitskonzept) ist Informationssicherheit ein fester Bestandteil der Agenda der regelmäßigen IT-Ausschusstreffen. Der/Die IT-Sicherheitsbeauftragte berichtet über den aktuellen Stand und erhält seine/ihre Aufgaben basierend auf den Entscheidungen des IT-Ausschusses.

Der Senat ist vor Erlass von IT-Sicherheitsrichtlinien ins Benehmen zu setzen.

JedeR Beschäftigte der Hochschule ist in seinem Wirkungsbereich für die Einhaltung des Informationssicherheitsniveaus als InformationseigentümerIn oder –bearbeiterIn verantwortlich.

§5 Informationsklassifizierung

Jede Art von Information wird von dem/der InformationseigentümerIn entsprechend der IT-Sicherheitsrichtlinie Informationsklassifikation eingeordnet. Dies erfolgt entsprechend ihres Wertes und ihrer Sensibilität zur Entwicklung eines angemessenen Sicherheitsniveaus.

§6 Zugriff auf Informationen und Daten

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

Alle BenutzerInnen von Applikationen/IT-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. Die Notwendigkeit, Art und Weise der Protokollierung bestimmt der/die InformationseigentümerIn.

§7 Sicherheitsbewusstsein

Das geforderte Maß an Informationssicherheit kann nur erreicht werden, wenn die beschäftigten Personen auf Informationssicherheitsbedrohungen 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.

§8 Gefahrenintervention/Sicherheitsvorfälle

Bei Gefahr der Verletzung der IT-Sicherheit kritischer Systeme der Hochschule können einE ServiceverantwortlicheR des Rechenzentrums gemeinsam mit dem/der CIO, die sofortige, vorübergehende Stilllegung des betroffenen IT-Systems anordnen, sowie die verantwortlichen BenutzerInnen vorübergehend von der Nutzung der Informationstechnik ausschließen.

Der Umgang mit Sicherheitsvorfällen erfolgt entsprechend einem dokumentierten Prozess zur Behandlung von IT-Sicherheitsvorfällen.

Der IT-Ausschuss bestimmt die IT-Dienste, für die der/die zentrale IT-Sicherheitsbeauftragte Notfallpläne sammelt und koordiniert. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen.

§9 Inkrafttreten

Diese Satzung tritt am Tage nach ihrer Bekanntmachung in Kraft.

Ausgefertigt aufgrund des Beschlusses des Senats vom 11.07.2017 und der Genehmigung des Präsidenten der Hochschule Augsburg vom 27.10.2017.

Augsburg, den 27.10.2017

Prof. Dr. Gordon T. Rohrmair

Präsident

Die Satzung wurde am 25.11.2017 an der Hochschule niedergelegt; die Niederlegung wurde am 25.11.2017 durch Aushang in der Hochschule bekanntgegeben.

Tag der Bekanntmachung ist der 25.11.2017.