hochschule aschaffenburg
university of applied sciences

Leitlinie
zur Informationssicherheit
an der Hochschule Aschaffenburg

Präambel

Der Betrieb einer Hochschule hängt in hohem Maße von der Qualität ihrer IT-Dienstleistungen ab. Das Vertrauen der Benutzerinnen und Benutzer in die Informationstechnik bildet die Grundlage für den erfolgreichen Einsatz. Um dieses Vertrauen zu rechtfertigen, müssen Integrität, Vertraulichkeit und Verfügbarkeit der IT-Dienste und Daten sichergestellt sein. Damit die Hochschule dieser Verantwortung nachkommen kann, müssen sämtliche Einrichtungen den Schutz der IT-Dienste und Daten 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 und
(4) gesetzliche Verpflichtungen (z. B. aus dem bayerischen Datenschutzgesetz) erfüllt werden können.

§ 1 Gegenstand der Leitlinie

Dieses Dokument definiert Grundsatzregelungen für folgende Informationssicherheitsziele:

(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 und Nutzer in und außerhalb der Hochschule
(4) Gewährleistung der Erfüllung der aus den gesetzlichen Vorgaben resultierenden Anforderungen an den Datenschutz
(5) Vorbeugende Maßnahmen zum Schutz vor und Minimierung der Schäden durch Sicherheitsvorfälle

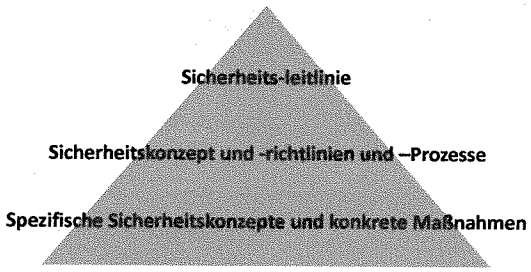
§ 2 Geltungsbereich

Diese Leitlinie erstreckt sich auf die gesamte Informationstechnik sowie sämtliche Anwenderinnen und Anwender, die diese benutzen oder bereitstellen. Sie ist damit verbindlich für alle Mitglieder, Einrichtungen sowie Dienstleisterinnen und Dienstleister der Hochschule.

§ 3 Informationssicherheitsmanagement

Das Informationssicherheitsmanagementsystem umfasst alle erforderlichen organisatorischen und technischen Maßnahmen um einen im Sicherheitskonzept zu definierenden 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 die 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. dienst-spezifischen Sicherheitskonzepten dokumentiert.



Die Sicherheitsrichtlinien umfassen mindestens folgende Bereiche:

(1) Organisation der IT-Sicherheit
(2) Bestimmung der Informationswerte (Informationsklassifikation)
(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

Die oder der zentrale IT-Sicherheitsbeauftragte ist für den Ablauf des Informationssicherheitsmanagementsystems verantwortlich. Sie oder er berät das Rechenzentrum, den Userbeirat sowie die IT-Beauftragten der Fakultäten und erarbeitet im Bedarfsfall Entscheidungsvorlagen für die Hochschulleitung.

Mit regelmäßigen Prüfungen der Umsetzung des Sicherheitskonzepts in allen Bereichen der Hochschule und Weiterentwicklung der Maßnahmen sorgt sie oder er für adäquate Informationssicherheit.

Von der Hochschule angebotene Dienste, die von außerhalb des Hochschulnetzes erreichbar sind, bedürfen der Prüfung und Freigabe durch die IT-Sicherheits- sowie ggf. die Datenschutzbeauftragte bzw. durch den IT-Sicherheits- oder Datenschutzbeauftragten.

§ 4 Informationssicherheitsverantwortung

Die Lenkungsverantwortung für das Informationssicherheitsmanagementsystem liegt beim Userbeirat. Die oder der IT-Sicherheitsbeauftragte handelt im Auftrag des Userbeirats und koordiniert methodisch das Informationssicherheitsmanagementsystem.

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

Zur kontinuierlichen Weiterentwicklung der Leitlinie und abhängiger Dokumente (Sicherheitskonzept) ist die Informationssicherheit ein fester Bestandteil der Agenda der regelmäßigen Treffen des Userbeirats. Die oder der IT-Sicherheitsbeauftragte berichtet über den aktuellen Stand und erhält ihre bzw. seine Aufgaben basierend auf den Entscheidungen des Userbeirats.

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

Jede Beschäftigte bzw. jeder Beschäftigte der Hochschule ist in seinem oder ihren Wirkungsbereich für die Einhaltung des Informationssicherheitsniveaus als Informationseigentümerin oder Informationseigentümer bzw. Informationsbearbeiterin oder Informationsbearbeiter verantwortlich.

§ 5 Informationsklassifikation

In der IT-Sicherheitsrichtlinie „Informationsklassifikation" werden Informationen nach Kriterien wie Schutzbedürftigkeit und Vertraulichkeit klassifiziert. Eigentümerinnen oder Eigentümer von Informationen ordnen Ihre Informationen entsprechend ihres Wertes und ihrer Sensibilität in diese Klassifikation ein.

§ 6 Zugriff auf Informationen und Daten

Der Zugriff auf Daten und IT-Systeme wird durch technische und organisatorische Maßnahmen und Prozesse ausreichend, dem Wert und der Bedeutung entsprechend, gesteuert. Alle Benutzerinnen oder Benutzer 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 sollen durch angemessene Protokollierung und Dokumentation nachvollziehbar sein. Die Notwendigkeit, Art und Weise der Protokollierung bestimmt die Informationseigentümerin bzw. der Informationseigentümer.

§ 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 regelmäßig zur Kenntnis gebracht.

§ 8 Gefahrenintervention/Sicherheitsvorfälle

Bei Gefahr der Verletzung der IT-Sicherheit kritischer Systeme der Hochschule können eine Serviceverantwortliche oder ein Serviceverantwortlicher des Rechenzentrums gemeinsam mit dem oder der CIO bzw. einer vertretungsberechtigten Person die sofortige, vorübergehende Stilllegung des betroffenen IT-Systems anordnen sowie die verantwortlichen Benutzerinnen oder Benutzer vorübergehend von der Nutzung der Informationstechnik ausschließen.
Der Umgang mit Sicherheitsvorfällen erfolgt entsprechend einem dokumentierten Prozess zur Behandlung von IT-Sicherheitsvorfällen.
Der Userbeirat bestimmt die IT-Dienste, für die der oder die zentrale IT-Sicherheitsbeauftragte Notfallpläne sammelt und koordiniert. Sie enthalten technische und organisatorische Handlungsanweisungen in Gefahrensituationen und bei Störfällen.

§ 9 Inkrafttreten

Diese Leitlinie tritt am Tage nach ihrer Bekanntmachung in Kraft.
Angefertigt im Benehmen mit dem Senat (Sitzung vom 17.01.2018).

Aschaffenburg, den 24.01.2018

Prof. Dr. Wilfried Diwischek
Präsident

Die Leitlinie wurde am 31.01.2018 niedergelegt. Die Niederlegung wurde am 31.01.2018 durch Rundmail in der Hochschule bekanntgegeben.

Tag der Bekanntmachung ist der 31.01.2018