Leitlinie

zur Informationssicherheit

an der Hochschule München

Präambel

Der Betrieb der Hochschule hängt in hohem Maße von der Qualität seiner IT-Dienstleistungen ab. Das Vertrauen 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 (Sicherheitsziele).

Damit die Hochschule dieser Verantwortung nachkommen kann, müssen sämtliche Beteiligte und Einrichtungen der Hochschule den Schutz der Informationstechnik unterstützen. Auf Grundlage dieser Leitlinie soll, zur Bewältigung der Aufgabe die erforderlichen Sicherheitsziele zu erreichen, hochschulweit ein Informationssicherheitsmanagementsystem (ISMS) etabliert 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 erfüllt werden können.

Absolute Informationssicherheit gibt es nicht. Die ergriffenen Maßnahmen -um die Sicherheitsziele zu erreichen- dienen dazu das verbleibende sogenannte Restrisiko möglichst zu minimieren. Die ergriffenen Maßnahmen sollen aber unter dem übergeordneten Handlungsaspekt noch wirtschaftlich vertretbar und mit Blick auf den maximal möglichen Schaden angemessen sein.

Mit Blick auf den hierfür erforderlichen Ressourcenbedarf zur Umsetzung an der Hochschule sind, wenn möglich, vorrangig Synergieeffekte durch hochschulübergreifende Zusammenarbeit zu nutzen. Beispielhaft ist die Nutzung von bundes- und bayernweiten hochschulspezifischen Empfehlungen und Richtlinien zu nennen.

§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 innerhalb und außerhalb der Hochschule.

(4) Gewährleistung der Erfüllung der aus den gesetzlichen Vorgaben resultierenden Anforderungen an den Datenschutz.

(5) Minimierung der Informationssicherheitsvorfälle und der ggf. daraus resultierenden Schäden.

§2 Geltungsbereich

Diese Leitlinie ist verbindlich für sämtliche Hochschulmitglieder und für alle organisatorischen Einheiten der Hochschule. Sie ist auch von der Hochschule beauftragten externen Dienstleistern und von der Hochschule München lizensierten oder zugekauften Informationstechnologien verpflichtend einzuhalten. Die Einhaltung kann durch einen Vorweis entsprechend anerkannter Informationssicherheitszertifikate und/oder dementsprechend detaillierten Beschreibungen von Maßnahmen zur Einhaltung der von der Hochschule geforderten Informationssicherheit nachgewiesen werden.

§3 Informationssicherheitsmanagementsystem

Das ISMS umfasst alle erforderlichen organisatorischen und technischen Maßnahmen um einen definierten Grad an Informationssicherheit (Sicherheitsniveau) zu erreichen und langfristig zu erhalten.

Um standardisierte Sicherheitsanforderungen für Geschäftsprozesse, Anwendungen und IT-Systeme zu erreichen, werden als Grundlage das „BSI IT-Grundschutz-Kompendium“ und das „IT-Grundschutzprofil für Hochschulen“ angewendet und auf die Bedarfe der Hochschule angepasst (Informationssicherheitskonzept). Diese Anforderungen beziehen sich auf interne und extern genutzte Informationstechnik. In der Anpassung auf die Bedarfe der Hochschule findet u.a. auch eine ausreichende Detaillierung der Anforderungen dieser Leitlinie und des erforderlichen Sicherheitsniveaus auch in Form von zwingend anzuwendenden Maßnahmen statt.

Grundsätzlich sind zur Erfüllung der Mindestsicherheitsanforderungen zunächst die Maßnahmen für die Basisanforderungen nach BSI Grundschutz zu erfüllen. Sollten die Sicherheitsanforderungen erhöhten Schutzbedarf erfordern, so muss eine geeignete

Risikobewertung erfolgen, um dann dementsprechende Maßnahmen zur Erfüllung des festgestellten Schutzbedarfes zu treffen.

§4 Informationssicherheitsverantwortung

Die Gesamtverantwortung für die Informationssicherheit an der Hochschule liegt bei der Hochschulleitung.

Der IT-Steuerkreis (IT-S) ist von der Hochschulleitung mit der Lenkungsverantwortung für das Informationssicherheitsmanagementsystem (ISMS) der Hochschule beauftragt und wird vom Chief Information Officer (CIO) der Hochschule geleitet. Der CIO berichtet regelmäßig an die Hochschulleitung über den Fortgang, der Einführung und den Betrieb des ISMS an der Hochschule.

Zur kontinuierlichen Weiterentwicklung der Leitlinie, abhängiger Dokumente, Prozesse und Organisation (Informationssicherheitskonzept), ist das Thema Informationssicherheit ein fester Bestandteil der Agenda der regelmäßigen Treffen des IT-S.

Der/Die Informationssicherheitsbeauftragte der Hochschule (ISB) ist für den Betrieb des ISMS verantwortlich. Er/Sie handelt im Auftrag des IT-S und berichtet regelmäßig an diesen. Der ISB berät den IT-S, die IT-Beauftragten der Fakultäten und Organisationseinheiten sowie die Zentrale IT.

Der ISB darf sich in diesem Zusammenhang Überblick über die IT-Sicherheit in allen Bereichen der Hochschule verschaffen.

Mit regelmäßigen Prüfungen der Umsetzung des Sicherheitskonzepts und Weiterentwicklung der Maßnahmen sorgt der ISB für adäquate Informationssicherheit.

Von der Hochschule angebotene Dienste, die von innerhalb und außerhalb des Hochschulnetzes erreichbar sind, bedürfen der Prüfung und Freigabe durch den ISB.

Eine Abweichung von den Mindestsicherheitsanforderungen eines Geschäftsprozesses, einer Anwendung und/oder eines IT-Systems nach BSI-Grundschutz, die einen sehr erhöhten Schutzbedarf erfordern, entscheidet die Hochschulleitung auf Basis der Empfehlung des IT-S über eine Einführung bzw. den Betrieb.

Die Umsetzungsverantwortung von erforderlichen Maßnahmen zur Erreichung eines erforderlichen Schutzbedarfs liegt beim Betreiber eines Geschäftsprozesses, einer Anwendung und/oder eines IT-Systems.

§5 Sicherheitsbewusstsein

Das geforderte Maß an Informationssicherheit kann nur erreicht werden, wenn die beschäftigten Personen auf Informationssicherheitsbedrohungen sensibilisiert und geschult sind, die eigenen Kompetenzen und Pflichten kennen und sich verantwortungsbewusst verhalten.

Sicherheitsrelevante Themen und Regeln werden den Hochschulangehörigen in geeigneten regelmäßigen Awareness-Schulungen und über andere hochschulweite Informationskanäle zur Kenntnis gebracht.

Jeder Hochschulangehörige ist in seinem Wirkungsbereich für die Einhaltung des Informationssicherheitsniveaus als InformationseigentümerIn oder –bearbeiterIn verantwortlich und ist verpflichtet regelmäßig an den von der Hochschule angebotenen Awareness-Schulungen zur Informationssicherheit teilzunehmen.

§6 Gefahrenintervention/Sicherheitsvorfälle

Bei erkennbarer erheblicher Gefahr der Verletzung der Informationssicherheit und/oder drohendem wirtschaftlichen Schaden oder Reputationsverlust, kann der ISB und/oder CIO und/oder Leiter der Zentralen IT die sofortige bzw. vorübergehende Stilllegung des betroffenen IT-Systems anordnen sowie die verantwortlichen BenutzerInnen vorübergehend von der Nutzung der Informationstechnik ausschließen. Die Hochschulleitung ist in diesem Fall unverzüglich zu informieren.

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

Der IT-S bestimmt die IT-Dienste, für die der ISB Notfallpläne sammelt und koordiniert. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen.

§7 Umsetzung

Diese Leitlinie bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, detaillierter Regelungen und Dienstanweisungen zur Informationssicherheit, die anzuwenden sind.

§8 Inkrafttreten

Diese Leitlinie tritt am Tage nach ihrer Bekanntmachung in Kraft.

Ausgefertigt aufgrund des Beschlusses der Hochschulleitung vom 17.12.2019. Genehmigung des Präsidenten der Hochschule München vom 18.12.2019.

München, den 18.12.2019

Prof. Dr. Martin Leitner
Präsident