Leitlinie
zur Informationssicherheit an der Technischen Hochschule Nürnberg Georg Simon Ohm

Version 2.2

Herausgeber:
Der Präsident der Technischen Hochschule Nürnberg Georg Simon Ohm
Keßlerplatz 12
90489 Nürnberg

Leitlinie
zur Informationssicherheit an der Technischen Hochschule Nürnberg Georg Simon Ohm

Präambel

In dieser Leitlinie zur Informationssicherheit werden die für alle Einrichtungen der Technischen Hochschule Nürnberg Georg Simon Ohm (TH Nürnberg) geltenden grundsätzlichen Ziele der Informationssicherheit festgelegt.

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.

Damit die Hochschule dieser 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 TH Nürnberg 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 bemisst sich an der Erreichung folgender Schutzziele für IT-Dienste und Daten[1]:

(1) Verfügbarkeit
Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

(2) Vertraulichkeit
Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

(3) Integrität
Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten bzw. Informationen und der korrekten Funktionsweise von Systemen.

(4) Authentizität
Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.

Die Erreichung dieser Schutzziele soll auf der Basis dieser Leitlinie zur Informationssicherheit durch ein Managementsystem zur Informationssicherheit (engl. Information Security Management System ISMS) sichergestellt werden. Das ISMS definiert Regeln und Verfahren, um die Informationssicherheit an der TH Nürnberg in einem fortlaufenden Prozess zu steuern, zu kontrollieren, aufrechtzuerhalten und kontinuierlich zu verbessern. Gleichzeitig ist die Erfüllung gesetzlicher Verpflichtungen, wie zum Beispiel des Bayerischen Datenschutzgesetz und der europäischen Datenschutzgrundverordnung, vorrangig zu gewährleisten.

[1] Definitionsbeschreibung lt. Bundesamt für Sicherheit in der Informationstechnik (BSI)

§1 Bezeichnungen

Der Begriff Informationssicherheit umfasst neben der Sicherheit der IT-Systeme (IT-Sicherheit) auch Daten, die nicht nur in elektronischer Form gespeichert und abgelegt werden.

Anstelle des Begriffs "IT-Sicherheit" tritt die Bezeichnung "Informationssicherheit", der bisherige IT-Sicherheitsbeauftragte erhält die Bezeichnung Informationssicherheitsbeauftragter (ISB).

Sofern in Dokumenten der Hochschule die Bezeichnungen "IT-Sicherheit", "IT-Sicherheitsbeauftragter" bzw. "IT-Sicherheitskonzept" verwendet werden, sind diese synonym zu den Begriffen "Informationssicherheit", "Informationssicherheitsbeauftragter" bzw. "Informationssicherheitskonzept" zu verstehen.

§2 Gegenstand der Leitlinie

Dieses Dokument drückt die Ausrichtung und Verantwortung der TH Nürnberg aus und 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 Nutzer in und außerhalb der TH Nürnberg.
(4) Gewährleistung der Erfüllung der aus den gesetzlichen Vorgaben resultierenden Anforderungen an den Datenschutz.
(5) Sicherstellung vorbeugender Maßnahmen, um das Auftreten von informationssicherheitskritischen Vorfällen zu minimieren.

§3 Geltungsbereich

Diese Leitlinie erstreckt sich auf die gesamte Informationstechnik der TH Nürnberg und sämtliche Hochschulangehörige und externe Anwender, die diese benutzen oder bereitstellen. Sie ist verbindlich für alle Organisationseinheiten der Hochschule. Externe Dienstleister oder Auftragnehmer werden bei Aufnahme der Vertragsbeziehungen auf Regelwerke des Informationssicherheitskonzepts schriftlich hingewiesen und auf dessen Beachtung verpflichtet.

§4 Informationssicherheitsmanagement

Das Managementsystem zur Informationssicherheit (ISMS) umfasst alle Anforderungen zum Umgang mit Informationen an der TH Nürnberg. Es umfasst alle angemessenen organisatorischen und technischen Maßnahmen, um für jeden bereitgestellten und genutzten Dienst, die Infrastruktur zur Informationsverarbeitung, Anwendungen sowie die zu verarbeitenden Daten einen unterschiedlich definierten Grad an Informationssicherheit (Sicherheitsniveau) zu erreichen und langfristig zu erhalten. Dazu ist entsprechend für jeden bereitgestellten und genutzten Dienst, Infrastruktur und Anwendung und Daten eine Klassifizierung gemäß des zu erreichenden Sicherheitsniveaus durchzuführen. Für Informationen, die aufgrund ihres Sicherheitsniveaus einen über einen Basisschutz hinausgehenden

Schutz erfordern, sind zusätzliche Maßnahmen auf Basis einer Risikoanalyse und -bewertung durchzuführen.

Der Informationssicherheitsbeauftragte überwacht den reibungslosen Ablauf des Informationssicherheitsprozesses und berichtet dazu an den Steuerkreis Informationssicherheit. Der Aufbau der Informationssicherheitsorganisation und die einzelnen Aufgaben des Informationssicherheitsbeauftragten sind in der anhängenden „Richtlinie zur Informationssicherheitsorganisation“ geregelt.

Dienste, die außerhalb der Hochschule erreichbar sind oder durch externe Dienstleister erbracht werden, bedürfen der Prüfung durch den Informationssicherheits- und Datenschutzbeauftragten.

Zur Erreichung eines angemessenen Sicherheitsniveaus sind die notwendigen Grundsätze, spezifische Regeln und Prinzipien in einem Sicherheitskonzept zu erfassen. Dort findet eine ausreichende Detaillierung der Anforderungen dieser Leitlinie und die angestrebten Sicherheitsniveaus je Informationssicherheitsziel in Form von Sicherheitsrichtlinien statt. Diese sind dann Basis für die erforderlichen individuellen Sicherheitsmaßnahmen. Die individuellen Maßnahmen sind in aufgabenspezifischen Umsetzungsanforderungen bzw. dienstspezifischen Sicherheitskonzepten dokumentiert und werden gemäß einem Informationssicherheitsprozess regelmäßig überprüft und ggf. an neue Bedrohungslagen angepasst.

Die Sicherheitsrichtlinien umfassen mindestens folgende Bereiche:

(1) Informationssicherheitsorganisation
(2) Bestimmung der Informationswerte (Klassifikation)
(3) Zugriffssteuerung, Netzwerk- und Betriebssicherheit
(4) IT-Systeme (wie Server, Speichersysteme, Arbeitsplatzrechner)
(5) Erkennen von Schwachstellen und Schutz vor Schadsoftware oder möglichen Angriffen
(6) Handhabung von Sicherheitsvorfällen
(7) Backup, Wiederherstellung und Notfallplanung
(8) Risikomanagement, Compliance und Datenschutz
(9) Physische Sicherheit
(10) Kommunikation

§5 Informationssicherheitsverantwortung

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

Die Hochschulleitung setzt dazu einen Steuerkreis Informationssicherheit ein, der den Informationssicherheitsprozess an der Hochschule verantwortet. Der Steuerkreis Informationssicherheit berät die Hochschulleitung in Fragen zur Informationssicherheit. Darüber hinaus ist er für die Aktualität der Informationssicherheitsrichtlinien verantwortlich.

Der Informationssicherheitsbeauftragte berät und handelt im Auftrag des Steuerkreises und koordiniert methodisch das Informationssicherheitsmanagement. Er gilt als zentraler Ansprechpartner in Fragen zur Informationssicherheit.

Jeder Beschäftigte der Hochschule ist in seinem Wirkungsbereich für die Einhaltung der Richtlinien, Maßnahmen und Anweisungen des Sicherheitskonzepts verantwortlich, um das jeweils geforderte Informationssicherheitsniveau gewährleisten zu können.

Die Leitungen aller Organisationseinheiten sind verantwortlich, dass allen Hochschulangehörigen die entsprechenden Richtlinien zur Informationssicherheit bekannt gemacht werden.

Die detaillierte Beschreibung der Verantwortung der einzelnen Rollen findet sich in der anhängenden „Richtlinie zur Informationssicherheitsorganisation“.

§6 Informationsklassifizierung

Die Grundlage des Informationsschutzes ist die Klassifizierung der IT-Systeme, Daten und Dokumente. Diese müssen entsprechend ihres Wertes und ihrer Sensibilität auf Basis der Informationssicherheitsrichtlinie und den dazugehörenden Konzepten (Schutzbedarfsfeststellung / Risikoanalyse) eingeordnet werden.

§7 Zugriff auf Informationen und Daten

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

Alle Benutzer von IT-Diensten/-Anwendungen/-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 Informationseigentümer in Abstimmung mit dem Datenschutzbeauftragten der TH Nürnberg.

§8 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.

Die Informationssicherheit gehört zu den Dienstpflichten aller Beschäftigten. Nur wenn alle Beteiligten das Verständnis für die getroffenen Sicherheitsmaßnahmen verinnerlichen und die Einhaltung der von sicherheitsrelevanten Maßnahmen als wertvoll und notwendig erkennen, kann ein geeignetes Niveau der Informationssicherheit erreicht werden.

§9 Gefahrenintervention/Sicherheitsvorfälle

Bei Gefahr der Verletzung der Informationssicherheit kritischer IT-Dienste/-Anwendungen/-Systeme der Hochschule können ein Serviceverantwortlicher des Rechenzentrums gemeinsam mit dem CIO, die sofortige, vorübergehende Stilllegung des betroffenen IT-Dienstes/-Anwendung/-Systems anordnen, sowie die verantwortlichen Benutzer vorübergehend von der Nutzung der Informationstechnik ausschließen.

Der Steuerkreis Informationssicherheit bestimmt die IT-Dienste/-Anwendungen/-Systeme, für die Notfallpläne sammelt und koordiniert werden. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen. Der Umgang mit Sicherheitsvorfällen erfolgt entsprechend einem dokumentierten Prozess zur Behandlung von IT-Sicherheitsvorfällen. Die dazugehörige Dokumentation enthält alle notwendigen Maßnahmen, Verantwortlichkeiten, Berichtswege und Eskalationsschritte, die vor, während bzw. nach einem derartigen Vorfall maßgeblich sind.

§10 Regelmäßige Audits

Die ständige Entwicklung und Modernisierung bei Hard- und Software und die steigende Anzahl neuer Bedrohungen informationsverarbeitender Systeme nicht nur aus dem Internet erfordern, dass die Verantwortlichen die Gültigkeit und Aktualität der Sicherheitsmaßnahmen regelmäßig auf das geforderte Sicherheitsniveau hin überprüfen. Diese Prüfungen sind, entsprechend der jeweils aktuell notwendigen Erfordernisse, Basis für ggf. zu ergreifende Maßnahmen zur Sicherstellung der Informationssicherheit an der TH Nürnberg.

Um das Sicherheitsniveau an der Hochschule messen zu können, werden Audits regelmäßig durch den Steuerkreis Informationssicherheit veranlasst.

§11 Finanzierung

Die Hochschule stellt im Rahmen ihrer Möglichkeiten den Beteiligten am Informationssicherheitsprozess ausreichend Mittel zur Verfügung, damit alle notwendigen Aufgaben und Maßnahmen umfassend und vollständig erfüllt werden können.

§12 Inkrafttreten

Diese Leitlinie zur Informationssicherheit für die TH Nürnberg tritt mit Unterzeichnung in Kraft.

Sie wird bei Inkrafttreten per Mail an die dienstlichen Mail-Adressen der Hochschulmitarbeiter bekannt gegeben und im Intranet veröffentlicht. Im Rahmen des Einstellungsprozesses werden neue Mitarbeiter auf diese Leitlinie zur Informationssicherheit und das Informationssicherheitskonzept hingewiesen.

Nürnberg, den 14.06.2018

gez.
Prof. Dr. Michael Braun
Präsident