IT-Sicherheitsleitlinie

für die Hochschule für angewandte Wissenschaften – Fachhochschule München (Hochschule München)

vom: 29. Juli 2010

Präambel

Die Hochschule München setzt für Arbeits- und Geschäftsprozesse in ihren Kernbereichen, anwendungsbezogener Forschung und Lehre und in ihrer Verwaltung verstärkt Informationstechnologien (IT) ein. Mit dem vermehrten Einsatz von IT-Lösungen, steigt auch die Abhängigkeit von deren Funktionsfähigkeit und die Gefahr potentieller wirtschaftlicher und sozialer Schäden durch IT-Risiken. Es ist daher für die Hochschule München von erheblichen strategischem Wert die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen durch entsprechende technische, strukturelle und personelle Maßnahmen zu schützen. Der Prozess orientiert sich an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

1. Gegenstand
   In dieser IT-Sicherheitsleitlinie soll zur Realisierung eines hochschulweiten IT-Sicherheitsprozesses, unter Berücksichtigung der einschlägigen gesetzlichen Bestimmungen die erforderlichen Verantwortungsstrukturen für die IT-Sicherheit festgelegt werden. Ferner formuliert sie Schutzziele und leitende Prinzipien der IT-Sicherheit an der Hochschule München.

2. Geltungsbereich
   Diese IT-Sicherheitsleitlinie gilt hochschulweit für alle Einrichtungen der Hochschule München (Fakultäten, wissenschaftliche Einrichtungen, Abteilungen und Bereiche der Zentralverwaltung und sonstige Einrichtungen) und in technischer Hinsicht für die gesamte IT-Infrastruktur inkl. der daran betriebenen IT-Systeme der Hochschule München. Sie gilt auch für außerhalb des Dienstgebäudes eingerichtete Arbeitsplätze (z. B. Telearbeitsplätze, mobile Arbeitsplätze, PC an Messeständen, etc.)

3. Schutzziele und Definitionen
   Schutzziele eines IT-Sicherheitsprozesses an der Hochschule München sind die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität von Informationen.

Alle Beschäftigten gewährleisten die IT-Sicherheit durch ihr verantwortliches Handeln und halten die für die IT-Sicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.

Definitionen:

- 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.*

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

- Integrität
  Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.*

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

  **Definitionsbeschreibung lt. Bundesamt für Sicherheit in der Informationstechnik (BSI), Glossar und Begriffsdefinitionen*

4. Verantwortlichkeiten und IT-Sicherheitsorganisation
   Die für den Einsatz und die Planung von IT-Projekten zuständigen Akteure oder Akteurinnen und deren Zuständigkeiten sind in der IT-Governance der Hochschule München vom 04. Juni 2008 sowie im Bayerischen Hochschulgesetz (BayHSchG) vom 23. Mai 2006 und der Grundordnung der Hochschule für angewandte Wissenschaften – Fachhochschule München vom 7. Dezember 2007 in ihren jeweils gültigen Fassungen festgelegt.
   Am IT-Sicherheitsprozess sind verantwortlich beteiligt:

   - Präsidium
     Das Präsidium trägt die Gesamtverantwortung für den IT-Sicherheitsprozess.

   - Erweiterte Hochschulleitung (EHL)
     Gemäß der IT-Governance ist die EHL höchste Entscheidungsinstanz in allen Fragen der IT-Sicherheit.

- IT-Steuerkreis (ITS)
  Der IT-Steuerkreis ist im Auftrag der EHL für die strategische Ausrichtung in IT-Fragen der gesamten Hochschule München verantwortlich. Er ist Entscheidungsinstanz für IT-Vorhaben mit bereichsübergreifendem Charakter und IT-Großprojekte. Er prüft und entscheidet abschließend über alle auf IT- Projekte gerichteten Ausgaben.

- Abteilung Zentrale IT
  Die Zentrale IT erbringt oder beauftragt IT-Basisdienste und überwacht deren Qualität.

- IT-Sicherheitsbeauftragte/r
  Der oder die IT-Sicherheitsbeauftragte wird vom Kanzler oder der Kanzlerin der Hochschule München bestellt. Er/Sie ist Mitglied im IT-Arbeitskreis. Zu seinen/ihren Kernaufgaben gehören:
  - Unterstützung des ITS bei der Entwicklung und Fortschreibung des IT-Sicherheitsprozesses;
  - Erstellung der notwendigen Regelwerke zum IT-Sicherheitsprozess und deren Vorlage beim ITS zur Beschlussfassung;
  - Sicherstellung der Umsetzung des IT-Sicherheit Regelwerkes in den Einrichtungen der Hochschule München;
  - Information des ITS über den Ablauf und die Integration des IT-Sicherheitsprozesses;
  - Koordination von Untersuchungen evtl. auftretender sicherheitsrelevanter Ereignisse;
  - Beratung der Fakultäten und sonstigen Einrichtungen zu Fragestellungen der IT-Sicherheit;
  - Gestaltung von Ausbildungs- und Sensibilisierungsmaßnahmen von Mitarbeitern und Mitarbeiterinnen;
  - Unterstützung des oder der Datenschutzbeauftragten bei Verfahrensfreigaben.

  Zur Wahrnehmung seiner/ihrer Aufgaben hat der oder die IT-Sicherheitsbeauftragte ein uneingeschränktes Zugriffsrecht auf alle sicherheitsrelevanten Informationen und Systeme und ein grundsätzliches Zutrittsrecht zu allen Einrichtungen der Hochschule München. Bei Gefahr in Verzug und wenn ein gravierender Schaden für die Hochschule München zu befürchten ist, kann er/sie Weisungen zur vorübergehenden Einstellung von IT-Anwendungen erteilen. Die getroffenen Weisungen bedürfen einer umgehenden nachträglichen Genehmigung durch den Kanzler oder die Kanzlerin oder in dessen oder deren Abwesenheit durch den Leiter oder die Leiterin der Zentralen IT.

- Bereichsleitung
  Die Leitung eines Bereiches der Hochschule (Fakultät, Abteilung, Zentralverwaltung etc.) ist für den gemäß IT-Governance laufenden IT-Einsatz in ihrem Aufgabenbereich verantwortlich.

- IT-Verfahrensverantwortliche
  Der IT-Einsatz an der Hochschule München wird in IT-Verfahren zusammengefasst, die IT-Verfahren werden dokumentiert und beschrieben und im Hinblick auf ihren Schutzbedarf analysiert. Für alle Verfahren wird vom ITS ein Verfahrensverantwortlicher oder eine Verfahrensverantwortliche benannt. Der oder die Verfahrensverantwortliche definiert den Schutzbedarf für das Verfahren.

- IT-Arbeitskreis (ITA)
  Im ITA erfolgt die hochschulweite Abstimmung von IT-Projekten.

5. IT-Sicherheitsprinzipien
   Folgende Prinzipien liegen dem IT-Sicherheitsprozess an der Hochschule München zugrunde:

   - Anwenderinnen und Anwender haben ein Grundverständnis für Belange der IT-Sicherheit;
   - IT-Systeme werden in einer sicheren Umgebung betrieben;
   - Informationen (Systeme, Daten etc.) werden adäquat vor unberechtigten Zugriffen geschützt;
   - Es werden Maßnahmen getroffen, um IT-Systeme vor schädlicher Software (sog. „Malware“) zu schützen;
   - IT-Systeme werden auf einem adäquaten Versionsstand gehalten;
   - Die administrative Arbeit auf IT-Systemen wird sicher und nachvollziehbar gestaltet;
   - Informationen werden ihrer Kritikalität entsprechend angemessen sicher verarbeitet;
   - IT-Systeme werden durch kompetentes Personal langfristig betreut;
   - Die Wirksamkeit der Schutzmaßnahmen wird regelmäßig überprüft und dokumentiert;
   - IT-Sicherheitszwischenfälle werden dokumentiert und geeignet kommuniziert.

6. Aufbau des Regelwerkes zur IT-Sicherheit
   Das Regelwerk zur IT-Sicherheit setzt sich aus dieser IT-Sicherheitsleitlinie sowie den allgemeinen und den produktspezifischen IT-Sicherheitsrichtlinien zusammen.
   Die allgemeinen Sicherheitsrichtlinien beschreiben detailliert dienst-/ zielgruppenbezogene Maßnahmen, die für einen Basisschutz vor Gefährdungen umgesetzt werden müssen.
   Die produktspezifischen Sicherheitsrichtlinien legen Sicherheitsmaßnahmen fest die getroffen werden müssen, um definierte Produkte oder Systeme sicher zu machen.

7. Information der MitarbeiterInnen und externer DienstleisterInnen
   Innerhalb der Fakultäten und sonstigen Einrichtungen der Hochschule München ist sicherzustellen, dass alle Mitarbeiter und Mitarbeiterinnen diese IT-Sicherheitsleitlinie und alle sonstigen Teile des IT-Regelwerkes sowie eventuelle Aktualisierungen kennen und im Rahmen Ihres Verantwortungsbereiches beachten. Externe Dienstleister und Dienstleisterinnen oder Auftragsnehmer und Auftragnehmerinnen werden bei Aufnahme der Vertragsbeziehungen auf das Regelwerk zur IT-Sicherheit schriftlich hingewiesen und auf dessen Beachtung pflichtet.

8. Aktualisierung
   Diese IT-Sicherheitsleitlinie sowie die sonstigen Richtlinien des Regelwerkes sind alle zwei Jahre sowie bei Bedarf durch insbesondere den oder die IT-Sicherheitsbeauftragten auf ihre Aktualität zu prüfen und gegebenenfalls fortzuschreiben.

9. Verstöße gegen das Regelwerk der IT-Sicherheit
   Verstöße gegen das Regelwerk können nach den allgemeinen Regelungen und gesetzlichen Bestimmungen insbesondere denen des Arbeits- und Disziplinarrechts geahndet werden und außerdem zu zivilrechtlichen oder strafrechtlichen Konsequenzen führen.
   Als Verstöße werden insbesondere angesehen:
   - Die Kompromittierung der Sicherheit von Informationen;
   - Der unberechtigte Zugriff auf Informationen;
   - Die unberechtigte Änderungen, Nutzung und/oder Veröffentlichung von Informationen.

10. Inkrafttreten
    Diese Sicherheitsleitlinie tritt am 29.07.2010 in Kraft.

Hochschule für angewandte Wissenschaften – Fachhochschule München

München, den ……

……
Prof. Dr. Michael Kortstock
Präsident