IT-Sicherheitsleitlinie der Fachhochschule Frankfurt am Main –
University of Applied Sciences
In der Fassung vom 09.02.2009
verabschiedet vom Präsidium am 09.02.2009

Präambel

Diese Leitlinie beschreibt, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Fachhochschule Frankfurt am Main hergestellt werden soll. Sie beinhaltet die von der Fachhochschule Frankfurt am Main angestrebten Informationssicherheitsziele, die Organisationsstrukturen, Aufgabenzuordnungen und die verfolgte Sicherheitsstrategie. Sie bildet damit das Fundament für die Sicherheitsstandards an der Hochschule und die sich daraus abgeleiteten Sicherheitsrichtlinien, Prozesse und Maßnahmen.

Zum Schutz der IT-Infrastruktur sind dieses Dokument und die daraus abgeleiteten Sicherheitsrichtlinien, Prozesse und Maßnahmen für alle Nutzer der IT-Infrastruktur der FH Frankfurt am Main verbindlich. Die Verbindlichkeit ist rechtlich erforderlich. Zum einen gibt es spezielle rechtliche Bestimmungen, wie z.B. zum Datenschutz, deren Einhaltung nur mit entsprechenden IT-Sicherheitsstandards gewährleistet werden kann. Zum anderen sind die Verantwortlichen der Hochschule unabhängig von speziellen Vorschriften zur IT-Sicherheit zur Abwehr von absehbaren Gefahren und Schäden verpflichtet. Erhebliche Schäden für die Hochschule sind möglich, z.B. durch Hacker-Angriffe, bei Vernichtung von wichtigen Daten oder Arbeitsausfall über einen längeren Zeitraum durch Ausfall der IT-Infrastruktur. Darüber hinaus muss mit nachfolgenden Schadensersatzforderungen geschädigter Dritter gerechnet werden. Zur Vorbeugung solcher Schäden gilt es mindestens die „verkehrsübliche Sorgfalt“ einzuhalten, um sich nicht dem Vorwurf des schuldhaften Handelns auszusetzen, zu dem auch eine mangelhafte Organisation zählt.

1 Einleitung

Eine funktionierende und sichere IT-Infrastruktur ist eine zentrale Grundlage für die Leistungsfähigkeit unserer Hochschule. Forschung, Lehre und Verwaltung sind von der Nutzung dieser Infrastruktur abhängig. Daher muss die Verfügbarkeit der Infrastruktur und die Vertraulichkeit und Integrität der dort gehaltenen relevanten Daten sichergestellt werden. Bedrohungen der Vertraulichkeit, Integrität und Verfügbarkeit ergeben sich durch Schwachstellen in den eingesetzten Systemen, die beispielsweise zu einem Ausfall eines wichtigen Rechners und dem Verlust der dort gespeicherten Informationen führen können oder es einem Hacker ermöglichen, durch einen vorsätzlichen Angriff unbefugten Zugriff auf einen Rechner zu erhalten und die dort gespeicherten Daten zu lesen oder zu manipulieren. Neben möglicherweise hohem finanziellen Schaden droht durch solche Angriffe auch ein bedeutender Imageverlust für die Hochschule.

Um diesem erheblichen Gefährdungspotential zu begegnen, ist es notwendig, die IT-Systeme vor Angriffen zu schützen und sicherzustellen, dass der Ausfall eines Systems in einem akzeptablen Zeitfenster und ohne den Verlust schützenswerter Daten kompensiert werden kann. Aufgrund der Komplexität der Materie und der sich rasch verändernden Technologien ist hierzu ein hochschulweit einheitlicher und kontinuierlicher IT-Sicherheitsprozess notwendig. Bei der Entwicklung und Umsetzung von Sicherheitsrichtlinien, Prozessen und Maßnahmen müssen Angemessenheit, Wirtschaftlichkeit und die besonderen Bedingungen an einer Hochschule berücksichtigt werden.

Somit sind

– organisatorische Rahmenbedingungen zur nachhaltigen Gewährleistung von IT-Sicherheit zu schaffen,

– ein IT-Sicherheitsmanagement einzurichten,

– abgestimmte Sicherheitsstandards einschließlich der Definition von Verantwortlichkeiten und Befugnissen zu erarbeiten,

– Komponenten zur Steigerung der IT-Sicherheit zu zentralisieren und standardisieren und alle Sicherheitsvorkehrungen und -maßnahmen hinreichend zu dokumentieren.

Die Hochschule orientiert ihren IT-Sicherheitsprozess an den vom Bundesamt für Sicherheit in der Informationstechnik entwickelten Standards und Grundsätzen.

2 Der IT-Sicherheitsprozess an der Fachhochschule Frankfurt am Main

2.1 Geltungsbereich

Der IT-Sicherheitsprozess erstreckt sich auf alle Einrichtungen der Hochschule (Fachbereiche, wissenschaftliche Einrichtungen, zentrale Einrichtungen und sonstige Einrichtungen), auf die gesamte IT-Infrastruktur der Hochschule, einschließlich der darin betriebenen IT-Systeme sowie der Gesamtheit der Benutzer. Eingeschlossen sind auch Aninstitute und Einrichtungen außerhalb der Hochschule, die direkt an das Hochschulnetz angeschlossen sind oder die Mitnutzer des Internetanschlusses der FH sind. Der IT-Sicherheitsprozess ist hochschulweit einheitlich. Der IT-Sicherheitsprozess umfasst nach festzulegenden Prioritäten technische und organisatorische Maßnahmen sowohl präventiver als auch reaktiver Art und Maßnahmen zur schnellen Krisenintervention.

2.2 IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie beschreibt allgemeinverständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Hochschule hergestellt werden soll. Sie beinhaltet die angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Sicherheitsleitlinie beschreibt damit auch die Sicherheitsziele und das angestrebte Sicherheitsniveau in der Hochschule.

2.3 IT-Sicherheitskonzept

Zum Erreichen der in der IT-Sicherheitsleitlinie festgeschriebenen Ziele wird ein IT-Sicherheitskonzept entworfen und umgesetzt. Im Rahmen dieses Verfahrens sind die personalvertretungsrechtlichen Beteiligungsrechte zu wahren. Nach IT-Grundschutz basiert die Erstellung des Konzepts auf einem Soll-Ist-Vergleich zwischen den bisher realisierten und den durch eine Modellierung ermittelten notwendigen organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen. Hierzu wird eine Strukturanalyse des bestehenden IT-Verbundes durchgeführt und der Ist-Zustand der Systeme ermittelt. Der Schutzbedarf der Systeme wird bestimmt und mit Hilfe der IT-Grundschutzkataloge ein Modell des IT-Verbunds erstellt. Dabei wird zwischen den Schutzbedarfskategorien „niedrig“, „normal“, „hoch“ und „sehr hoch“ differenziert, die unterschiedliche notwendige Maßnahmen zum Schutz der Systeme erfordern. Durch einen

Soll-Ist-Vergleich zwischen dem Modell und dem tatsächlichen Status wird identifiziert, welche Maßnahmen noch umzusetzen sind. Je nach Schutzbedarf der Systeme sind ggf. zusätzliche Schritte wie eine Risikoanalyse oder andere ergänzende Sicherheitsanalysen notwendig. Die umzusetzenden Maßnahmen werden dann konsolidiert, priorisiert und realisiert. Diese Vorgehensweise ist kontinuierlich fortzuführen.

2.4 IT-Sicherheitsrichtlinien

Sicherheitsrichtlinien bilden das Regelwerk für den Betrieb einzelner Komponenten der IT-Struktur. Sie werden anhand der im Sicherheitskonzept definierten Standards formuliert und realisiert. Die Sicherheit soll besonders durch Anwendung von Verfahren und Tools nach dem jeweiligen Stand der Technik erreicht werden. Die Abteilung Datenverarbeitung stellt eine Liste der vorhandenen Sicherheitsrichtlinien bereit und erstellt bzw. aktualisiert sie je nach Erforderlichkeit. Die Einhaltung der Sicherheitsrichtlinien ist verbindlich. Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des IT-Betriebes und der IT-Sicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.

2.5 Kontrolle

Die Wirksamkeit der Sicherheitsmaßnahmen ist regelmäßig zu kontrollieren.

3 Leitlinien der IT-Sicherheit

Die IT-Sicherheit an der Fachhochschule Frankfurt orientiert sich an folgenden Grundsätzen:

- Die FH Frankfurt ist bestrebt, eine offene IT-Infrastruktur zu betreiben und einen offenen Informationsaustausch zu gewährleisten, sofern keine dienst-, urheber- und datenschutzrechtlichen Belange verletzt werden.
- Unter IT-Sicherheit wird der Schutz von Informationen und Informationssystemen gegen unbefugte Zugriffe und Manipulationen sowie die Sicherstellung der Verfügbarkeit der durch die Systeme bereitgestellten Dienste für legitime Benutzer verstanden. Sie umfasst somit die Verhinderung von inneren und äußeren Angriffen auf die interne IT-Infrastruktur, die Verhinderung von Angriffen aus der internen IT-Infrastruktur auf Systeme externer Institutionen, die Verhinderung von Ausfällen von IT-Diensten und die Sicherung der in der IT-Infrastruktur gehaltenen und verarbeiteten Daten gegen vorsätzliches oder unabsichtliches Löschen oder Verfälschen.
- Für den IT-Einsatz sind die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit im jeweils erforderlichen Maße zu erreichen.
- In Abwägung der Werte der zu schützenden Informationen, der Risiken sowie des Aufwands an Personal und Finanzmitteln für IT-Sicherheit soll für eingesetzte und geplante IT-Systeme in der Fachhochschule Frankfurt ein angemessenes IT-Sicherheitsniveau angestrebt und erreicht werden:
    - Die IT-Sicherheit ist kein Selbstzweck. Sie muss stets die Verhältnismäßigkeit der Maßnahmen und Mittel im Spannungsfeld zwischen Informationsoffenheit, Kosten und Nutzerakzeptanz auf der einen und dem notwendigen Grad von Sicherheit auf der anderen Seite berücksichtigen.

- Die hieraus abgeleiteten Sicherheitsmaßnahmen sind auch dann anzuwenden, wenn sich daraus Beeinträchtigungen für die IT-Nutzung ergeben.

- Viele Beeinträchtigungen der IT-Sicherheit beruhen auf allgemein bekannten Schwachstellen, die bei sachgemäßer Handhabung und Organisation mit vertretbarem Aufwand und ohne signifikante Benutzerbeeinträchtigung zu beseitigen sind.

- Die Sicherheit der IT-Verfahren ist neben der Leistungsfähigkeit und Funktionalität zu gewährleisten. Eine absolute Sicherheit der IT-Infrastruktur ist jedoch nicht realisierbar. Bleiben im Einzelfall trotz der Sicherheitsvorkehrungen Risiken untragbar, ist an dieser Stelle auf den IT-Einsatz zu verzichten.

- IT-Sicherheit kann nur erreicht werden, wenn hochschulweit einheitliche Sicherheitsstandards definiert und umgesetzt werden. Hierfür ist ein dynamischer, prozessorientierter und kontinuierlicher Ablauf notwendig.

- Die Durchsetzung, Aufrechterhaltung und dauerhafte Fortentwicklung der IT-Sicherheitsstandards wird durch die Tatsache gewährleistet, dass das Präsidium den IT-Sicherheitsprozess initiiert und aktiv unterstützt.

- Die Hochschule orientiert ihren IT-Sicherheitsprozess an den vom Bundesamt für Sicherheit in der Informationstechnik entwickelten Standards und Grundsätzen.

- IT-Sicherheit ist eine Gemeinschaftsaufgabe, die von allen Nutzern der IT-Infrastruktur wahrgenommen werden muss. Die Nutzer werden für Belange der IT-Sicherheit sensibilisiert und über das Gefährdungspotential und mögliche Gegenmaßnahmen in ihrem Arbeitsumfeld informiert. Alle Nutzer gewährleisten die IT-Sicherheit durch ihr verantwortliches Handeln und halten die für die IT-Sicherheit relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen ein.

- Die Sicherheitsstandards sind kontinuierlich weiter zu entwickeln und durch Qualitätssicherungsmaßnahmen zu ergänzen, durch die zeitnah neue Risiken erkannt und geeignete Gegenmaßnahmen ergriffen werden können.

4 Organisationsstruktur und Verantwortlichkeiten

4.1 Verantwortlichkeiten

Die Bedeutung, die der Informationstechnik zukommt, und der einrichtungsübergreifende Charakter des IT-Sicherheitsprozesses bedingen, dass der gesamte Komplex der IT-Sicherheit in den Kompetenz- und Verantwortungsbereich des Präsidiums fällt. Alle Nutzer der IT der Hochschule sind dafür verantwortlich, dass die IT-Sicherheitsprozesse eingehalten und die festgelegten Sicherheitsmaßnahmen in ihrem Bereich umgesetzt werden. Unterstützt durch sensibilisierende Schulungen und Benutzerbetreuung am Arbeitsplatz soll jeder im Rahmen seiner Möglichkeiten Sicherheitsvorfälle von innen und außen vermeiden. Sicherheitsrelevante Ereignisse sind den Zuständigen umgehend zu melden, damit schnellstmöglich Abhilfemaßnahmen eingeleitet werden können.

Die jeweils Zuständigen für Daten, Informationen und Verfahren sowie für unterstützende Systeme sind verpflichtet, bei der Erstellung und Änderung von Sicherheitskonzepten und

Sicherheitsrichtlinien mitzuwirken sowie das Sicherheitskonzept und die jeweiligen Sicherheitsrichtlinien zu beachten und umzusetzen. Änderungen der Richtlinien, beispielsweise aufgrund neuer technischer Entwicklungen oder neuer Bedrohungen, sind zeitnah umzusetzen.

Ein Auftragnehmer (vgl. § 4 HDSG), der für die Verwaltung Leistungen erbringt, hat Vorgaben des Auftraggebers zur Einhaltung der IT-Sicherheitsziele (Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Verbindlichkeit) gemäß dieser IT-Sicherheitsleitlinie einzuhalten. Der Auftraggeber hat Sicherheitsanforderungen vertraglich festzulegen und deren Einhaltung zu kontrollieren. Der Auftraggeber hat den Auftragnehmer zu verpflichten, bei erkennbaren Mängeln oder Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren.

Die Einhaltung der IT-Sicherheit bei der Verarbeitung, Nutzung und Kontrolle von Daten und Informationen ist zu überprüfen. Art und Umfang der Kontrolle sind vom Präsidium auf der Grundlage des jeweiligen Sicherheitskonzeptes festzulegen. Eine Kontrolle kann durch unabhängige Dritte erfolgen. In diesem Fall ist zu gewährleisten, dass keine unzulässige Kenntnisnahme von Daten und Informationen damit verbunden ist.

4.2 Gesamtorganisation, Beauftragte und Gremien

Am IT-Sicherheitsprozess der Hochschule werden folgende Gremien und Funktionsträger verantwortlich beteiligt:

- der/die IT-Sicherheitsbeauftragte der Fachhochschule,
- das IT-Sicherheitsmanagement-Team (SMT),
- die Abteilung Datenverarbeitung,
- die Fachbereiche,
- die Verwaltungsabteilungen, Referate und andere Einrichtungen.

Das Präsidium setzt einen IT-Sicherheitsbeauftragten ein. Das Präsidium setzt außerdem ein IT-Sicherheitsmanagement-Team (SMT) ein. Ständige Mitglieder des SMT sind:

- der Kanzler als Vertreter des Präsidiums,
- der IT-Beauftragte des Präsidiums,
- der IT-Sicherheitsbeauftragte,
- der Datenschutzbeauftragte,
- der Leiter der Abteilung Datenverarbeitung,
- die IT-Beauftragten der Fachbereiche und Einrichtungen.

Die Dekane der Fachbereiche und die Leiter der Einrichtungen der Hochschule sind für den Betrieb und die Sicherheit der IT-Systeme in ihren jeweiligen Bereichen verantwortlich. Jeder Fachbereich und jede Einrichtung der Hochschule benennt einen IT-Beauftragten und einen Stellvertreter, der für den Betrieb und die Sicherheit in der jeweiligen Einheit zuständig ist. Dabei kann ein IT-Beauftragter für mehrere Einrichtungen zuständig sein.

4.3 Aufgaben der Beteiligten und Umsetzung des IT-Sicherheitsprozesses

Der IT-Sicherheitsbeauftragte ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Institution. Er berät das Präsidium in Fragen der Informationssicherheit und unterstützt sie bei der Umsetzung. Seine Aufgaben umfassen unter anderen:

- den Informationssicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,

- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- die Realisierung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- der Leitungsebene und dem SMT über den Status quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- Sicherheitsvorfälle zu untersuchen und
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und koordinieren.

Der IT-Sicherheitsbeauftragte ist außerdem bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben, sowie bei der Einführung neuer Anwendungen und IT-Systeme zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten.

Das SMT unterstützt den IT-Sicherheitsbeauftragten, indem es übergreifende Maßnahmen in der Hochschule koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt. Aufgaben des SMT sind insbesondere:

- Informationssicherheitsziele und -strategien zu bestimmen sowie die Leitlinie zur Informationssicherheit zu entwickeln,
- die Umsetzung der Sicherheitsleitlinie zu überprüfen,
- den Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
- bei der Erstellung des Sicherheitskonzepts mitzuwirken,
- zu überprüfen, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen wie beabsichtigt funktionieren sowie geeignet und wirksam sind,
- die Schulungs- und Sensibilisierungsprogramme für Informationssicherheit zu konzipieren sowie
- das strategische IT-Team und das Präsidium in Fragen der Informationssicherheit zu beraten.

Die Abteilung Datenverarbeitung ist für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit verantwortlich, die in Form von Sicherheitsrichtlinien hochschulweit bekanntgemacht werden. Hierzu zählt auch die Definition von Prozessen zur Gewährleistung der IT-Sicherheit. Es arbeitet in diesen Bereichen eng mit dem IT-Sicherheitsbeauftragten zusammen.

Die am IT-Sicherheitsprozess Beteiligten arbeiten in allen Belangen der IT-Sicherheit zusammen, stellen die dazu erforderlichen Informationen bereit und regeln die Kommunikations- und Entscheidungswege sowohl untereinander wie auch in Beziehung zu Dritten. Hierbei ist insbesondere der Aspekt der in Krisensituationen gebotenen Eile zu berücksichtigen.

Alle Nutzer der IT der Hochschule sind zur Meldung sicherheitsrelevanter Ereignisse verpflichtet.

5 Gefahrenintervention und -vorbeugung

5.1 Gefahrenintervention

Bei Gefahr im Verzug können die Abteilung Datenverarbeitung, der IT-Sicherheitsbeauftragte und die IT-Beauftragten in ihrem Bereich die sofortige vorübergehende Stilllegung betroffener IT-Systeme und/oder Netzwerkanschlüsse veranlassen, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist. Die Leiter der entsprechenden Bereiche, der IT-Sicherheitsbeauftragte und das SMT sind unverzüglich zu informieren.

Die Wiederinbetriebnahme nach vorübergehender Stilllegung kann erst nach Durchführung hinreichender Sicherheitsmaßnahmen erfolgen. Die Maßnahmen werden zwischen dem IT-Sicherheitsbeauftragten, der Abteilung Datenverarbeitung und dem Leiter der betroffenen Einrichtung abgestimmt.

5.2 Vorsorgemaßnahmen

Notfallpläne sollen Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse beinhalten, mit dem Ziel, Gefahren soweit möglich abzuwenden sowie eine hinsichtlich des Schutzbedarfs der entsprechenden Systeme möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen zu erreichen. Es sind Notfallpläne für wichtige Dienste in allen Einrichtungen der Hochschule, insbesondere für zentrale Dienste in der Abteilung Datenverarbeitung zu erarbeiten und fortzuschreiben. Die Wirksamkeit von Notfallplänen ist durch Notfallübungen zu überprüfen.

6 Verstöße und Folgen

Verhalten, das die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährdet, kann disziplinar- oder arbeitsrechtlich geahndet werden. Unter Umständen kann das Verhalten als Ordnungswidrigkeit oder als Straftat verfolgt werden. Als Straftat kommen insbesondere in Betracht:

– das unbefugte Verschaffen von Daten anderer, die gegen unberechtigten Zugang besonders gesichert sind (§§ 202a, 274 Abs. 1 Nr. 2 StGB)

– der Computerbetrug durch unrichtige Gestaltung eines Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder durch unbefugte Einwirkung auf den Ablauf (§ 263a StGB)

– die fälschliche Beeinflussung einer Datenverarbeitung (§§ 270, 269 StGB), das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (§ 303a StGB)

– das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers (§ 303b StGB)

– die Verwendung personenbezogener Daten entgegen den Vorschriften des HDSG (§ 40 HDSG).

Beschäftigte, die die Sicherheit von Daten, Informationen, IT-Systemen oder des Netzes gefährden und einen Schaden für das Land oder einen Dritten verursachen, können darüber hinaus zum Schadenersatz (§ 91 HBG, § 14 BAT, § 823 BGB) herangezogen werden oder einem Rückgriffanspruch (Art. 34 GG i.V.m. § 839 BGB) ausgesetzt sein.

7 Sonstiges

7.1 Finanzierung

Die personellen und finanziellen Ressourcen für alle erforderlichen IT-Sicherheitsmaßnahmen in einer Einrichtung der Hochschule sind von der betreffenden Einrichtung zu erbringen. Darunter fallen auch Schulungskosten für Administratoren und Benutzer der Einrichtung.

Die personellen und finanziellen Ressourcen aller zentralen IT-Sicherheitsmaßnahmen sind aus zentralen Ansätzen zu finanzieren.

7.2 In-Kraft-Treten

Diese Leitlinie tritt nach ihrer Verabschiedung am Tag nach ihrer Bekanntmachung in Kraft. Sie ersetzt die IT-Sicherheitsordnung in der Fassung vom 7.6.2005.