IT-Sicherheitsordnung für die Hochschule Magdeburg-Stendal (FH) vom 14.02.2007

Inhaltsverzeichnis:

Präambel

Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit einer Hochschule auf den Gebieten Lehre und Forschung. Der Hochschulbetrieb erfordert in zunehmenden Maß die Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Informationstechnik (IT) stützen. Dafür ist aber die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten zwingend erforderlich.

Unter diesen Bedingungen kommt der „Sicherheit in der Informationstechnik“ („IT-Sicherheit“) eine grundsätzliche und strategische Bedeutung in der Hochschule zu. Hauptziel der Gestaltung von IT-Sicherheit muss es sein, den entsprechenden Rahmen für das Funktionieren von Lehre und Forschung zu bieten.

Dieses kann wegen der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten und wegen der begrenzten finanziellen und personellen Möglichkeiten nur in einem kontinuierlichen IT-Sicherheitsprozess erfolgen, der den besonderen Bedingungen der Hochschule Magdeburg-Stendal (FH) gerecht wird.

Ziel von IT-Sicherheitsmaßnahmen ist es, nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern primär die in der Hochschule Magdeburg-Stendal (FH) verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen zu schützen sowie die Hochschule soweit möglich vor Imageverlust und finanziellen Schäden zu bewahren. Die Entwicklung und Fortschreibung des IT-Sicherheitsprozess muss sich einerseits an den gesetzlich festgelegten Aufgaben der Hochschulen sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren, andererseits ist sie nur über einen kontinuierlichen IT-Sicherheitsprozess innerhalb geregelter Verantwortungsstrukturen zu erzielen. Es empfiehlt sich diesen IT-Sicherheitsprozess an Prinzipien zu orientieren, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutzhandbuch niedergelegt sind.

Die vorliegende IT-Sicherheitsordnung regelt die Zuständigkeiten und die Verantwortung sowie die

Zusammenarbeit in einem hochschulweiten IT-Sicherheitsprozess.

§ 1
Gegenstand der Ordnung

Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines hochschulweiten IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen, eine grobe Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten. Diese Ordnung wird ergänzt durch die separate Ordnung für die Benutzung der IT-Infrastrukturen der Hochschule Magdeburg-Stendal (FH) (Benutzungsordnung für Informationsverarbeitungssysteme der Fachhochschule Magdeburg; 9.6.99).

§ 2
Geltungsbereich

Der Geltungsbereich dieser Ordnung erstreckt sich auf die gesamten Einrichtungen der Hochschule Magdeburg-Stendal (FH) (Fachbereiche, wissenschaftliche Einrichtungen, zentrale Einrichtungen und sonstige Einrichtungen), auf die gesamte IT-Infrastruktur der Hochschule Magdeburg-Stendal (FH), einschließlich der daran betriebenen IT-Systeme sowie der Gesamtheit der Benutzer (Gäste und Mitglieder).

§ 3
Beteiligte am hochschulweiten IT-Sicherheitsprozess

Die Hauptverantwortung für den IT-Sicherheitsprozess liegt bei der Hochschulleitung. Sie setzt daher folgende Gremien und Funktionsträger ein und bindet bestehende Einrichtungen in den IT-Sicherheitsprozess ein:

i. IT-Sicherheitsmanagement-Team (SMT)
ii. Dezentrale IT-Sicherheitsbeauftragte (Dies können sein: DV-Organisator(inn)en, Netzverantwortliche, sonstiges IT-Personal)
iii. Zentrum für Kommunikation und Informationsverarbeitung (ZKI)
iv. Einrichtungen und Gremien der Hochschule Magdeburg-Stendal (FH)

§ 4
Einsetzung der Beteiligten

(1) Die Hochschulleitung setzt ein IT-Sicherheitsmanagement-Team (SMT) ein. Die Zusammensetzung des SMT sollte – unter Beschränkung der Anzahl der Mitglieder auf das notwendige Maß– sowohl die unterschiedlichen Aufgabenbereiche der Hochschule Magdeburg-Stendal (FH) widerspiegeln als auch die unterschiedlichen, für die Hochschule relevanten Aspekte der IT-Sicherheit berücksichtigen. Ständige Mitglieder des SMT sind:

i. ein(e) Vertreter(in) der Hochschulleitung,
ii. der/die Datenschutzbeauftragte,
iii. ein(e) Vertreter(in) der dezentralen IT-Sicherheitsbeauftragten (siehe § 3),
iv. Leiter/-in des ZKI,
v. Leiter/-in der Kommission für Kommunikation und Informationsverarbeitung.

Weitere sachverständige Mitglieder werden in Abstimmung mit den Hochschulgremien von der Hochschulleitung benannt.

(2) Das SMT wählt aus dem Kreis der ständigen Mitglieder eine(n) Vorsitzende(n).

(3) Das SMT setzt zur Unterstützung seiner Arbeit im operativen Bereich eine Arbeitsgruppe ein. Sie setzt sich aus allen dezentralen IT-Sicherheitsbeauftragten und einem(r) Vertreter(in) des ZKI zusammen. Der(die) Leiter(in) dieser Arbeitsgruppe wird als Mitglied nach § 4 (1) iii bestellt. Bei Bedarf soll die Gruppe den Rat von Expert(inn)en einholen (z. B. Jurist(inn)en, Spezialist(inn)en für Teilbereiche der IT-Sicherheit).

(4) Jeder Fachbereich und jede Einrichtung der Hochschule Magdeburg-Stendal (FH) hat eine(n) dezentrale(n) IT-Sicherheitsbeauftragte(n) und eine(n) Stellvertreter(in) zu bestellen. Es kann aber auch ein(e) dezentrale(r) IT-Sicherheitsbeauftragte(r) für mehrere Einrichtungen zuständig sein. Durch die Benennung müssen alle IT-Systeme im Geltungsbereich sowie die für den Betrieb vor Ort verantwortlichen Personen einem(r) IT-Sicherheitsbeauftragten zugeordnet sein.

(5) Bei der Bestellung/Benennung der im IT-Sicherheitsprozess aktiven Personen soll die erforderliche personelle Kontinuität berücksichtigt werden. Deshalb sollen die IT-Sicherheitsbeauftragten über langfristige Verträge verfügen oder möglichst zum hauptamtlichen Personal der Hochschule gehören.

(6) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leitung der Einrichtungen nicht von ihrer Gesamtverantwortung für die IT-Sicherheit in ihrem Zuständigkeitsbereich.

§ 5
Aufgaben der Beteiligten

(1) Das SMT ist für die Richtlinienerstellung, Fortschreibung, Umsetzung und Überwachung des hochschulweiten IT-Sicherheitsprozesses verantwortlich. Unter anderem ist dabei das Erarbeiten von Notfallplänen zu berücksichtigen.

(2) Das SMT gibt die hochschulinternen technischen Standards zur IT-Sicherheit vor. Außerdem veranlasst es die Schulung und Weiterbildung der dezentralen IT-Sicherheitsbeauftragten und die Unterstützung bei der Richtlinienumsetzung.

(3) Das SMT dokumentiert sicherheitsrelevante Vorfälle und erstellt jährlich einen IT-Sicherheitsbericht.

(4) Der(die) Vorsitzende des SMT berät die Hochschulleitung in relevanten Fragen der IT-Sicherheit.

(5) Die dezentralen IT-Sicherheitsbeauftragten sind für die Umsetzung aller mit dem SMT abgestimmten Sicherheitsbelange bei den IT-Systeme und -Anwendungen sowie den Mitarbeiter(inne)n in ihren Verantwortungsbereichen (Systembetreiber lt. § 3 Absatz 2.b der „Benutzungsordnung für Informationsverarbeitungssysteme der Fachhochschule Magdeburg“) verantwortlich. Sie sind verpflichtet sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf einem aktuellen Stand zu halten.

(6) Das ZKI ist für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit zentraler Systeme (Systembetreiber lt. § 3 Absatz 2.a der „Benutzungsordnung für Informationsverarbeitungssysteme der Fachhochschule Magdeburg“) verantwortlich. Es arbeitet eng mit dem SMT zusammen.

(7) Die Einrichtungen der Hochschule Magdeburg-Stendal (FH) sind verpflichtet, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zu IT-Sicherheit die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten sowie das SMT zu beteiligen.

(8) 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.

§ 6
Umsetzung des IT-Sicherheitsprozesses

(1) Das SMT initiiert, steuert und kontrolliert die Umsetzung des hochschulweiten IT-Sicherheitsprozesses, der nach festzulegenden Prioritäten technische und organisatorische Maßnahme sowohl präventiver als auch reaktiver Art sowie Maßnahmen zur schnellen Krisenintervention umfassen muss.

(2) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Zuständigkeitsbereich verantwortlich. Dafür müssen sie vom SMT und der Leitung der jeweiligen Einrichtung mit entsprechenden Kompetenzen ausgestattet werden. Sie informieren regelmäßig sowohl die Leitung ihrer Einrichtung als auch das SMT über den Stand der Umsetzung und über aktuelle Problemfälle.

(3) Es sind Notfallpläne zu erarbeiten, die Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse beinhalten sollen, mit dem Ziel, Gefahren soweit möglich abzuwenden sowie eine möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen zu erreichen.

(4) Das SMT setzt einen Arbeitskreis ein, der primär als Basis dienen soll, um die Umsetzung des IT-Sicherheitsprozesses hochschulweit abzustimmen und Erfahrungen auszutauschen.

§ 7
Krisenintervention

(1) Bei Gefahr im Verzuge veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige vorübergehende Stilllegung betroffener IT-Systeme in ihrem Zuständigkeitsbereich, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist. Das SMT ist unverzüglich zu informieren.

(2) Soweit das ZKI Gefahr im Verzuge feststellt, kann es Netzanschlüsse (ggf. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur der Hochschule Magdeburg-Stendal (FH) in Teilen oder insgesamt nicht anders abzuwenden ist. Der(die) zuständige dezentrale IT-Sicherheitsbeauftragte sowie das SMT werden unverzüglich ggf. nachträglich informiert.

(3) Die Wiederinbetriebnahme erfolgt erst nach der Durchführung hinreichender IT-Sicherheitsmaßnahmen in Abstimmung mit dem SMT.

§ 8
Finanzierung

(1) Die personellen und finanziellen Ressourcen für alle erforderlichen IT-Sicherheitsmaßnahmen in einer Einrichtung der Hochschule Magdeburg-Stendal (FH) sind von der betreffenden Einrichtung zu erbringen. Darunter fallen auch die Schulungskosten für den/die dezentralen IT-Sicherheitsbeauftragten sowie die Benutzer der Einrichtung.

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

§ 9
Sonstige Regelungen

Mitbestimmungsrechte des Landespersonalvertretungsgestzes (LpersVG) werden beachtet. Regelungen, die mitbestimmungspflichtige Tatbestände enthalten, werden dem (Gesamtpersonalrat (GPR) rechtzeitig und unaufgefordert vor Inkrafttreten vorgelegt.

§ 10
Inkrafttreten

Diese Ordnung tritt am Tage nach Ihrer hochschulöffentlichen Bekanntmachung in den Amtlichen Bekanntmachungen der Hochschule Magdeburg-Stendal (FH) in Kraft.

Ausgefertigt aufgrund des Beschlusses des Senates der Hochschule Magdeburg-Stendal (FH) vom 14.02.2007.

Der Kanzler