Ordnung der Hochschule Bremen für die Sicherheit der Informationstechnik (IT-Sicherheitsordnung)
vom 19. Mai 2009

Die Rektorin der Hochschule Bremen hat am 25. Mai 2009 gemäß § 110 Absatz 3 des Bremischen Hochschulgesetzes (BremHG) in der Fassung der Bekanntmachung vom 9. Mai 2007 (Brem. GBl. S. 339) die vom Akademischen Senat am 19. Mai 2009 beschlossene IT-Sicherheitsordnung der Hochschule Bremen in der nachstehenden Fassung genehmigt.

Präambel

Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit einer Hochschule auf den Gebieten Lehre, Forschung und Verwaltung. Der Hochschulbetrieb erfordert in zunehmenden Maß die Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Informationstechnik (IT) stützen. Dafür ist 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, die die Entwicklung und Umsetzung einer einheitlichen hochschulweiten Rahmenrichtlinie der IT-Sicherheit für die Hochschule Bremen erforderlich macht. Hauptziel der Gestaltung von IT-Sicherheit muss es sein, den entsprechenden Rahmen für das Funktionieren von Lehre, Forschung und Verwaltung 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 gerecht wird.

Diese Ordnung regelt die Zuständigkeiten und die Verantwortlichkeit sowie die Zusammenarbeit im hochschulweiten IT-Sicherheitsprozess.
Ziel der IT-Sicherheitsordnung ist es nicht nur, die existierenden gesetzlichen Auflagen zu erfüllen, sondern primär die in der Hochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen zu schützen sowie die Hochschule Bremen 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) in den IT-Grundschutz-Katalogen niedergelegt sind.

Um den gestiegenen Anforderungen an IT-Sicherheit Rechnung zu tragen, ist die Initiierung eines IT-Sicherheitsprozesses notwendig. Dazu soll ein IT-Sicherheitsmanagement-Team (SMT) eingesetzt werden, das die IT Sicherheitsordnung als Grundlage seiner Tätigkeit nimmt. Der IT-Sicherheitsprozess startet mit einer Analysephase, in der die Ist-Situation des Informationsverbundes (Gebäude, Räume, IT-Systeme, Anwendungen, Netze) aufgenommen wird. Weiterhin wird zusammen mit den Einrichtungen ein Soll-Zustand festgelegt, der zum einen eine angemessene Informationssicherheit der Hochschule zum Ziel hat und zum anderen die Anforderungen der Einrichtungen der Hochschule berücksichtigt. Im nächsten Schritt werden die Maßnahmen festgelegt, um diesen Soll-Zustand vom SMT und den Einrichtungen der Hochschule umzusetzen. Bei der Umsetzung wird u.a. festgelegt welche Aufgaben und Kenntnisse der / die dezentrale IT-Sicherheitsbeauftragte hat. Dieser IT-Sicherheitsprozess orientiert sich an den Empfehlungen des DFN (Deutsches Forschungsnetz e.V.) und ZKI (Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V.) und basiert auf den Prinzipien, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in den IT-Grundschutz-Katalogen

niedergelegt sind. Die Frage, ob dabei eine BSI-Zertifizierung angestrebt werden soll, ist im Arbeitsprozess des SMT zu klären.

§ 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 Benutzungsordnung für Informationsverarbeitungssysteme der Hochschule Bremen.

§ 2
Geltungsbereich

Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Einrichtungen der Hochschule Bremen (Fakultäten, wissenschaftliche Einrichtungen, zentrale Einrichtungen, Verwaltung und sonstige Einrichtungen), auf die gesamte IT-Infrastruktur der Hochschule, einschließlich der darin betriebenen IT-Systeme sowie die Gesamtheit der Benutzer. Die Festlegungen dieser Ordnung und der hieraus entstehenden Konzepte müssen bei Vereinbarungen und Verträgen mit An-Instituten und externen Einrichtungen, die direkt an das Hochschulnetz angeschlossen sind oder über dieses Mitnutzer des Deutschen Forschungsnetzes (DFN) sind, Bedingung sein.

§ 3
Beteiligte am IT-Sicherheitsprozess

Die Verantwortung für den IT-Sicherheitsprozess liegt beim Rektorat. Die Verantwortlichkeit wird nach Maßgabe der nachfolgenden Bestimmungen durch das Rektorat abgestuft delegiert auf:

1. das IT-Sicherheitsmanagement-Team (SMT)
2. die dezentralen IT-Sicherheitsbeauftragten
3. das Rechenzentrum (RZhsb).

§ 4
Einsetzung der Beteiligten

(1) Die Hochschulleitung setzt ein IT-Sicherheitsmanagement-Team (SMT) ein.

Ständige Mitglieder des SMT sind:

- eine Vertreterin / ein Vertreter des Rektorats,
- die / der Datenschutzbeauftragte,
- eine Vertreterin / ein Vertreter der dezentralen IT-Sicherheitsbeauftragten,
- eine Vertreterin / ein Vertreter des RZhsb.

Weitere sachverständige Mitglieder können von der Hochschulleitung – auch befristet – benannt werden. Das Mitglied des Rektorats führt den Vorsitz.

(2) Nach Vorgabe des SMT werden dezentrale IT-Sicherheitsbeauftragte bestellt. In jeder Fakultät wird mindestens eine / ein IT-Sicherheitsbeauftragte/r bestellt. Durch die Benennung müssen alle IT-Systeme im Geltungsbereich sowie die für den Betrieb vor Ort verantwortlichen Personen einer/m IT-Sicherheitsbeauftragten zugeordnet sein.

(3) Bei der Bestellung/Benennung der im IT-Sicherheitsprozess aktiven Personen soll die erforderliche personelle Kontinuität berücksichtigt werden. Deshalb sollen die IT-Sicherheitsbeauftragten zum hauptamtlichen Personal der Hochschule Bremen gehören.

§ 5
Aufgaben der Beteiligten

(1) Das SMT ist für die Richtlinienerstellung, Fortschreibung, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich. Dazu zählt auch das Erarbeiten von Notfallplänen.

(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/operative Arbeitsgruppe dokumentiert sicherheitsrelevante Vorfälle und erstellt jährlich einen IT-Sicherheitsbericht.

(4) Die dezentralen IT-Sicherheitsbeauftragten sind für die Umsetzung aller mit dem SMT abgestimmten Sicherheitsbelange bei den IT-Systemen und -Anwendungen sowie den Mitarbeiterinnen und Mitarbeitern in ihren Verantwortungsbereichen verantwortlich. Sie sind verpflichtet sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf einem aktuellen Stand zu halten.

(5) Das RZhsb ist für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit verantwortlich. Es arbeitet eng mit dem SMT zusammen.

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

(7) 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. Bei Gefahr im Verzug für die IT-Sicherheit hat für alle Beteiligten die Beseitigung der IT-Sicherheitsrisiken Vorrang vor anderen Dienstaufgaben.

§ 6
Umsetzung des IT-Sicherheitsprozesses

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

(2) Die zu erarbeitenden Notfallpläne beinhalten Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse. Sie verfolgen das Ziel, Gefahren abzuwenden und eine möglichst schnelle Wiederherstellung der Verfügbarkeit betroffener IT-Ressourcen zu erreichen.

(3) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Zuständigkeitsbereich verantwortlich. Mit ihrer Bestellung erhalten sie die zur Wahrnehmung ihrer Aufgaben erforderlichen Befugnisse in ihrem Zuständigkeitsbereich. Sie informieren regelmäßig die Leitung ihrer Einrichtung über den Stand der Umsetzung und über aktuelle Problemfälle.

(4) Das SMT beruft einen Arbeitskreis aus dem Kreis der dezentralen IT-Sicherheitsbeauftragten, um die Umsetzung des IT-Sicherheitsprozesses hochschulweit abzustimmen und Erfahrungen auszutauschen.

(5) Alle Angehörigen und Mitarbeiter der Hochschule Bremen sowie alle Benutzer der IT-Infrastruktur sind zur Meldung sicherheitsrelevanter Ereignisse an die dezentralen IT-Sicherheitsbeauftragten oder an Mitglieder des SMT verpflichtet.

§ 7
Krisenintervention

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

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

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

§ 8
Finanzierung

(1) Die personellen und finanziellen Ressourcen für alle erforderlichen dezentralen IT-Sicherheitsmaßnahmen 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 Mitteln zu finanzieren.

§ 9
In-Kraft-Treten

Diese Ordnung tritt nach Genehmigung durch die Rektorin in Kraft.

Bremen, den 25. Mai 2009
Die Rektorin der Hochschule Bremen