14. Mai 2013

UniReport

Goethe-Universität | Frankfurt am Main Satzungen und Ordnungen

IT-Sicherheitsordnung der Goethe-Universität Frankfurt am Main

Beschluss des Präsidiums vom 7. Mai 2013 gemäß § 37 Abs. 8 Hessisches Hochschulgesetz vom 14. September 2009 in der geltenden Fassung (HHG, GVBL I S.666ff.)

Präambel

Der Betrieb einer Hochschule hängt in hohem Maße von der Qualität ihrer IT-Dienstleistungen ab. Das Vertrauen der Benutzerinnen und Benutzer in die Informationstechnik bildet die Grundlage für ihren erfolgreichen Einsatz. Integrität, Vertraulichkeit und Verfügbarkeit der IT-Dienste und Daten sind nachhaltig sicherzustellen. Um dieser Verpflichtung angesichts einer wachsenden Bedrohung der sich rasch weiterentwickelnden Technik bei gleichzeitig begrenzter personeller und finanzieller Ausstattung der Hochschule nachzukommen, müssen sämtliche Einrichtungen der Hochschule den Schutz der Informationstechnik als gemeinsame Herausforderung begreifen, die auf der Basis einer einheitlichen Rahmenrichtlinie der IT-Sicherheit der Hochschule in einem kontinuierlichen IT-Sicherheitsprozess angegangen wird. Unerlässliche Grundvoraussetzung für den Erfolg ist dabei ein Ausgleich zwischen den Anforderungen akademischer Freiheit und IT-Sicherheit.

§ 1 Gegenstand der Ordnung

Die IT-Sicherheitsordnung bestimmt die für den IT-Sicherheitsprozess der Goethe-Universität erforderliche Organisationsstruktur und definiert Aufgaben und Verantwortlichkeiten.

§ 2 Geltungsbereich

Die IT-Sicherheitsordnung erstreckt sich auf die gesamte Informationstechnik der Goethe-Universität in ihren wissenschaftlichen und nicht wissenschaftlichen Einrichtungen und gilt für sämtliche Benutzerinnen und Benutzer, die diese einsetzen oder bereitstellen. Sie ist verbindlich für die Fachbereiche und wissenschaftlichen, zentralen oder sonstigen Einrichtungen der Hochschule sowie von diesen mit der Wahrnehmung von IT-Dienstleistungen und sonstigen mit der IT-Sicherheit zusammenhängenden Tätigkeiten beauftragten Firmen oder Personen. Für den Bereich des Klinikums, speziell der Krankenversorgung, sollen gesonderte Regelungen gelten. Bis zu ihrem Erlass gilt diese Ordnung entsprechend.

§ 3 Beteiligte des IT-Sicherheitsprozess

Am IT-Sicherheitsprozess sind beteiligt:

(1) Präsidium der Universität
(2) zentrale IT-Sicherheitsbeauftragte
(3) IT-Sicherheits-Management-Team (SMT)
(4) dezentrale IT-Sicherheitsbeauftragte
(5) Personalrat der Hochschule
(6) behördliche Datenschutzbeauftragte der Universität
(7) Einrichtungen der Hochschule
(8) Hochschulrechenzentrum

§ 4 Einsetzung des zentralen IT-Sicherheitsbeauftragten

(1) Das Präsidium setzt eine zentrale IT-Sicherheitsbeauftragte oder einen zentralen IT-Sicherheitsbeauftragten ein, die oder der ihm unmittelbar berichtet.

(2) Jeder Fachbereich, wissenschaftliche, zentrale und sonstige Einrichtung der Hochschule benennt eine dezentrale IT-Sicherheitsbeauftragte oder einen dezentralen IT-Sicherheitsbeauftragten.

(3) Eine dezentrale IT-Sicherheitsbeauftragte oder ein

dezentraler IT-Sicherheitsbeauftragter kann für mehrere Einrichtungen und Fachbereiche zuständig sein.

(4) Die Aufgabenbereiche der dezentralen IT-Sicherheitsbeauftragten oder des dezentralen IT-Sicherheitsbeauftragten sind so zu regeln, dass jedem IT-System und jeder Benutzerin und jedem Benutzer eine dezentrale IT-Sicherheitsbeauftragte oder ein dezentraler IT-Sicherheitsbeauftragter zugeordnet wird.

(5) Die Benennung der dezentralen IT-Sicherheitsbeauftragten oder des dezentralen IT-Sicherheitsbeauftragten erfolgt ausschließlich aus dem hauptamtlichen Personal der Hochschule.

(6) Benennt eine Einrichtung keine IT-Sicherheitsbeauftragte oder keinen IT-Sicherheitsbeauftragten, kann das Präsidium eine kommissarische IT-Sicherheitsbeauftragte oder einen IT-Sicherheitsbeauftragten bestellen.

§ 5 IT-Sicherheits-Management-Team

(1) Das Präsidium richtet ein IT-Sicherheits-Management-Team ein. Seine Mitglieder sind:
- ein Vertreter des Präsidiums
- Leiter des Rechenzentrums
- zentrale Sicherheitsbeauftrage oder zentraler Sicherheitsbeauftragter
- ein Vertreter der dezentralen IT-Sicherheitsbeauftragten
- der behördliche Datenschutzbeauftragte der Universität

(2) Das IT-Sicherheits-Management-Team kann bei Bedarf erweitert werden um Experten für Betriebssysteme (z.B. Unix-, Linux oder Microsoft-Windows), fachlich Verantwortliche (z.B. E-Mail-, Netzwerk- oder Nutzeradministration) und Vertreter des Personalrats.

§ 6 Aufgaben der am IT-Sicherheitsprozess Beteiligten

(1) Das IT-Sicherheits-Management-Team bildet für die Hochschule das zentrale Beschluss- und Kontrollorgan über die IT-Sicherheit. Es verfasst und beschließt die einheitliche Rahmenrichtlinie der IT-Sicherheit der Hochschule und erstellt jährlich einen IT-Sicherheitsbericht. Die einheitliche Rahmenrichtlinie der IT-Sicherheit ist mit dem Ziel einer Verständigung rechtzeitig und eingehend mit dem Personalrat zu erörtern.

(2) Die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte ist für die Umsetzung der Rahmenrichtlinie der IT-Sicherheit an der Hochschule verantwortlich und wird darin vom IT-Sicherheits-Management-Team unterstützt. Die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte ist in allen sicherheitsrelevanten Fragen Ansprechpartnerin oder Ansprechpartner nach innen und nach außen. Sie oder er dokumentiert sicherheitsrelevante Vorfälle und entwickelt einen Schulungs- und Weiterbildungsplan zur IT-Sicherheit.

(3) Die dezentralen IT-Sicherheitsbeauftragten sind für die Durchführung des IT-Sicherheitsprozesses in ihrer Einrichtung verantwortlich.

(4) Das Rechenzentrum unterstützt die IT-Sicherheitsbeauftragten und das IT-Sicherheits-Management-Team in technischen Fragen.

(5) Trotz der Benennung der dezentralen IT-Sicherheitsbeauftragten bleibt die Verantwortung der Leitungen der Fachbereiche, wissenschaftlichen, zentralen und sonstigen Einrichtungen für die IT-Sicherheit in ihrem Bereich unberührt. Sie sind verpflichtet, an allen Planungen, Verfahren und Entscheidungen in Bezug zur IT-Sicherheit die zuständige dezentrale IT-Sicherheitsbeauftragte oder den zuständigen dezentralen IT-Sicherheitsbeauftragten und die zentrale IT-Sicherheitsbeauftragte oder den zentralen IT-Sicherheitsbeauftragten zu beteiligen.

(6) Die am IT-Sicherheitsprozess Beteiligten arbeiten in allen Belangen der IT-Sicherheit zusammen. Bei Bedarf können exter-

ne Fachleute beratend hinzugezogen werden.

§ 7 Umsetzung des IT-Sicherheitsprozesses

(1) Die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte konzipiert ein hochschulweites Informations- und Kommunikationssystem, über das alle Beteiligte am IT-Sicherheitsprozess in Kontakt stehen.

(2) Die dezentralen IT-Sicherheitsbeauftragten sind verpflichtet, sich aktuelle sicherheitsrelevante Informationen zu beschaffen und werden darin vom der zentralen IT-Sicherheitsbeauftragten oder von dem zentralen IT-Sicherheitsbeauftragten unterstützt. Die dezentralen Sicherheitsbeauftragten veranlassen in ihrem Bereich die erforderlichen IT-Sicherheitsmaßnahmen zur Gefahrenabwehr. Hierzu müssen sie von der Leitung ihrer Einrichtung mit den notwendigen Kompetenzen ausgestattet werden.

(3) Die am IT-Sicherheitsprozess Beteiligten informieren sich gegenseitig unverzüglich, umfassend und vollständig über sicherheitsrelevante Vorfälle. Über jeden Vorfall muss die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte informiert werden.

(4) Die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte darf sämtliche für den IT-Sicherheitsprozess relevanten Informationen, die bei dessen Durchführung in den einzelnen Einrichtungen anfallen, einholen. Erfolgt die Einholung in datenschutzerhebliche Informationen, ist dies zu dokumentieren und die betroffene Benutzerin oder der betroffene Benutzer gegebenenfalls nach Zweckerreichung unverzüglich zu benachrichtigen. Werden arbeitsplatz- und personalbezogene Daten von Hochschulbeschäftigten benötigt, ist der Personalrat darüber in Kenntnis zu setzen.

Der behördliche Datenschutzbeauftragte der Universität soll auf schriftlichen Antrag von beeinträchtigten Benutzerinnen oder Benutzern überprüfen, ob die Informationseinholung für den IT-Sicherheitsprozess relevant und notwendig war. Der behördliche Datenschutzbeauftragte informiert den/ die Antragssteller/ Antragsstellerin und das IT-Sicherheits-Management-Team über die Ergebnisse der Überprüfung und kann Empfehlungen für die zukünftige Informationseinholung aussprechen.

(5) Das IT-Sicherheits-Management-Team tagt regelmäßig, mindestens einmal pro Semester. Es soll Vorschläge zur Weiterentwicklung der Rahmenrichtlinie der IT-Sicherheit, die Beteiligten am IT-Sicherheitsprozess können hierzu dem IT-Sicherheitsmanagement-Team Vorschläge unterbreiten.

§ 8 Gefahrenintervention

(1) Bei einem Verstoß gegen die IT-Sicherheitsordnung oder die einheitliche Richtlinie der IT-Sicherheit der Hochschule kann die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte die sofortige, vorübergehende Stilllegung des betroffenen IT-Systems anordnen sowie die verantwortlichen Benutzerinnen und Benutzer vorübergehend von der Nutzung der Informationstechnik ausschließen. Die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte muss unverzüglich den zuständigen dezentralen IT-Sicherheitsbeauftragten oder die zuständige dezentrale Sicherheitsbeauftragte über den Vorgang informieren. Vorübergehende Stilllegungen sollen erst nach vorheriger erfolgloser Abmahnung erfolgen, wenn die Gefahrenlage diese vor der Stilllegung zulässt. Der/dem Betroffenen ist Gelegenheit zur Stellungnahme zu geben, wenn dies vorher möglich ist. Andernfalls kann der/die Betroffene nach der Stilllegung eine Stellungnahme abgeben.

(2) Bei Gefahr in Verzug kann das Rechenzentrum Netzanschlüsse vorübergehend sperren, wenn ein dro-

hender hoher Schaden von der Hochschule durch andere geeignete Maßnahmen nicht abgewendet werden kann. Das Rechenzentrum muss unverzüglich die zentrale IT-Sicherheitsbeauftragte oder den zentralen IT-Sicherheitsbeauftragten und den zuständigen dezentralen IT-Sicherheitsbeauftragten oder die zuständige dezentrale Sicherheitsbeauftragte über den Vorgang informieren.

(3) Die Wiederinbetriebnahme vorübergehend stillgelegter IT-Systeme setzt deren eingehende Überprüfung und Freigabe durch die zuständige dezentrale Sicherheitsbeauftragte oder den zuständigen dezentralen IT-Sicherheitsbeauftragten voraus.

(4) Nach Rücksprache mit dem IT-Sicherheits-Management-Team hebt die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte den Ausschluss einer oder eines vorübergehend von der Nutzung der Informationstechnik gesperrten Benutzerin oder Benutzers wieder auf, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint. Eine dauerhafte Nutzungseinschränkung eines IT-Systems kommt nur bei schwerwiegenden oder wiederholten Verstößen gemäß Absatz 1 in Betracht, wenn trotz vorherigen Mahnungen auch künftig ein ordnungsgemäßer Betrieb nicht mehr zu erwarten ist. Die Entscheidung trifft die Präsidentin oder der Präsident auf Antrag der zentralen IT-Sicherheitsbeauftragten oder des zentralen IT-Sicherheitsbeauftragten durch Bescheid. Weitere mögliche Ansprüche der Hochschule sowie des Systembetreibers aus dem Nutzungsverhältnis bleiben unberührt.

(5) Das IT-Sicherheits-Management-Team bestimmt IT-Dienste, für die zentrale IT-Sicherheitsbeauftragte oder der zentrale IT-Sicherheitsbeauftragte Notfallpläne erstellt. Sie enthalten Handlungsanweisungen in Gefahrensituationen und bei Störfällen und unterteilen sich in einen allgemein zugänglichen Benachrichtigungsplan und in ein detailliertes Notfallkonzept für den Dienstgebrauch.

§ 9 Finanzierung

Die Hochschule muss den am IT-Sicherheitsprozess Beteiligten ausreichend Mittel zur Verfügung stellen, damit diese ihre Aufgaben unverzüglich, umfassend und vollständig erfüllen können.

§ 10 Inkrafttreten

Die IT-Sicherheitsordnung tritt nach Beschlussfassung des Präsidiums nach ihrer Veröffentlichung in Kraft.

Frankfurt, den 7. Mai 2013

gez.
Prof. Dr. Enrico Schleiff

Impressum
UniReport Satzungen und Ordnungen erscheint unregelmäßig und anlassbezogen als Sonderausgabe des UniReport. Die Auflage wird für jede Ausgabe separat festgesetzt.

Herausgeber Der Präsident der Johann Wolfgang Goethe-Universität Frankfurt am Main