UNIVERSITÄT SIEGEN

Amtliche Mitteilungen

Datum **26. Juli 2011** **Nr. 25/2011**

I n h a l t :

Leitlinien zur Informationssicherheit der Universität Siegen

Vom 26. Juli 2011

Herausgeber: Rektorat der Universität Siegen
Redaktion: Dezernat 3, Herrengarten 3, 57068 Siegen, Tel. 0271/740-4813

Leitlinie
zur
Informationssicherheit
der
Universität Siegen

Vom 26. Juli 2011

Auf der Grundlage der Ordnung zum Datenschutz und zur IT-Sicherheit an der Universität Siegen vom 06. Dezember 2006 (Amtliche Mitteilung 41/2006), in der Fassung des Beschlusses des Senats vom 21. November 2007, hat das Rektorat folgende Leitlinie zur Informationssicherheit beschlossen:

1. Präambel

Leistungsfähige Forschung und Lehre an der Universität Siegen stützen sich verstärkt auf die Möglichkeiten der Informationstechnik (IT), daher bilden funktionierende und sichere IT-Prozesse und Dienstleistungen eine zentrale Grundlage und bedingen somit die Sicherstellung der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen, Systemen und Diensten gemäß den Standards des Bundesamtes für Sicherheit und der Informationstechnik (BSI) und den Empfehlungen der Zentren für Kommunikation und Informationsverarbeitung in Forschung und Lehre e.V. (ZKI).

Die Informationssicherheit (IT-Sicherheit) umfasst im Allgemeinen eine Vielzahl von Aspekten, neben technischen und infrastrukturellen Rahmenbedingungen vor allem auch organisatorische Maßnahmen und Regelungen, in denen u. a. auch datenschutzrechtliche Kriterien berücksichtigt werden.

Auf dem Weg zu einem integrierten Informationsmanagement an der Universität Siegen kommt der IT-Sicherheit eine grundsätzliche und strategische Bedeutung zu, die die Entwicklung und Umsetzung einer einheitlichen hochschulweiten Leitlinie zur IT-Sicherheit erforderlich macht. Dieses kann wegen der heterogenen IT-Landschaft, der sich schnell weiter entwickelnden technischen Möglichkeiten und aufgrund der begrenzten finanziellen und personellen Rahmenbedingungen nur in einem kontinuierlichen IT-Sicherheitsprozess erfolgen.

Die Aufgabe der IT-Sicherheitsleitlinie ist nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern vor allem die verarbeitenden Systeme, übertragenen und gespeicherten Daten und Anwendungen zu schützen, sowie die Universität Siegen soweit möglich vor Imageverlust und finanziellen Schäden zu bewahren.

Diese Leitlinie basiert auf der Ordnung zum Datenschutz und zur IT-Sicherheit an der Universität Siegen vom 6. Dezember 2006, die vom Senat verabschiedet wurde, und beschreibt konkretisierend den Informationssicherheitsprozess an der Universität Siegen. Sie dient als Grundlage für das hochschulweite IT-Sicherheitskonzept. Die daraus resultierenden Maßnahmen sollen eine größtmögliche Sicherheit im Umgang mit IT gewährleisten. Für eine erfolgreiche Umsetzung des IT-Sicherheitsprozesses ist ein Ausgleich zwischen akademischer Freiheit und IT-Sicherheit notwendig. Die Grundvoraussetzungen werden dabei durch klare Verantwortungsstrukturen sowie durch die Unterstützung aller Mitglieder und Angehörigen der Universität Siegen gebildet.

2. Geltungsbereich

Diese Leitlinie zur Informationssicherheit gilt für alle Einrichtungen der Universität Siegen (Fakultäten, Zentrale Universitätsverwaltung, Universitätsbibliothek, sowie weitere wissenschaftliche und Service - Einrichtungen), für die gesamte IT-Infrastruktur, einschließlich der in den Einrichtungen betriebenen IT-Systeme und IT-Dienste, sowie für alle Mitglieder, Angehörige und Gäste der Universität Siegen.

Ziele

Aus den allgemein anzustrebenden Schutzzielen der Informationssicherheit wie Verfügbarkeit, Integrität und Vertraulichkeit werden die folgenden IT-Sicherheitsziele für die Universität Siegen abgeleitet:

- Schutz der Verfügbarkeit von IT-Systemen, Diensten und Daten,
- Sicherstellung der Vertraulichkeit bei der Verarbeitung von Informationen und Daten,
- Schutz der Integrität der IT-Systeme, Dienste und Daten,
- Schutz vor unberechtigtem Zugriff auf Daten und Systeme,
- Sensibilisierung der Hochschulangehörigen für einen sicheren Umgang mit IT,

- Aufbau eines Notfallmanagements,
- Ermittlung von Sicherheitsrisiken mit anschließender Definition von geeigneten Gegenmaßnahmen,
- Einhaltung der einschlägigen Gesetze und sonstigen rechtlichen Bestimmungen und
- Wahrung der Persönlichkeitsrechte der Mitarbeiterinnen/Mitarbeiter und der Studierenden, sowie weiterer Angehöriger der Hochschule.

3. Organisation und Aufgaben

Die nachfolgenden Personen bzw. Gremien werden maßgeblich an dem IT-Sicherheitsprozess beteiligt:

CIO-Gremium

Die Aufgabe des CIO-Gremiums ist die strategische Entwicklung der IT-basierten Dienstleistungen im Sinne eines integrierten Informationsmanagements. Das CIO-Gremium berät das Rektorat und wird vom CIO geleitet. Dem CIO-Gremium gehören folgende Personen an:

- CIO,
- Rektor/in und Kanzler/in als Vertreter des Rektorats,
- die Leiter/innen der zentralen Einheiten ZIMT, Zentrale Universitätsverwaltung und Universitätsbibliothek, die IT-basierte Dienstleistungen anbieten und
- der/die Sprecher/in des Nutzergremiums.

Das CIO-Gremium wird fallspezifisch von der/dem Datenschutzbeauftragten und der/dem IT-Sicherheitsbeauftragten beraten.

Datenschutzbeauftragte/r

Die/der Datenschutzbeauftragte gemäß Abschnitt 2.1. der Ordnung zum Datenschutz und zur IT-Sicherheit ist Ansprechpartner/in in allen Fragen des Datenschutzes an der Universität Siegen und berät neben dem CIO-Gremium primär die datenverarbeitenden Stellen bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten.

Sie/er ist bei der Erarbeitung behördeninterner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten frühzeitig zu beteiligen und hat die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen und die mit der Verarbeitung personenbezogener Daten befassten Personen mit den Bestimmungen des Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen.

IT-Sicherheitsbeauftragte/r

Die/der IT-Sicherheitsbeauftragte (CISO) gemäß Abschnitt 3.1.1 der Ordnung zum Datenschutz und zur IT-Sicherheit wird von der Hochschulleitung bestellt und berät die Hochschulleitung, das CIO-Gremium, die einzelnen Organisationseinheiten und die/den Datenschutzbeauftragten in allen Fragen der IT-Sicherheit. Die Aufgaben beinhalten neben der Koordination und Steuerung des IT-Sicherheitsprozesses die Erstellung von Richtlinien und Regelungen sowie die Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zur IT-Sicherheit. Des Weiteren ist sie/er für die Initiierung und Überprüfung der Umsetzung von IT-Sicherheitsmaßnahmen verantwortlich. Sie/er ist frühzeitig bei Erarbeitung von sicherheitsrelevanten Projekten und Konzepten einzubeziehen. Die/der IT-Sicherheitsbeauftragte leitet das IT-Sicherheitsteam und erstellt in Zusammenarbeit mit diesem ein hochschulweites IT-Sicherheitskonzept.

Die/der IT-Sicherheitsbeauftragte und die/der Datenschutzbeauftragte arbeiten bei themenübergreifenden Fragestellungen in den Bereichen Informationssicherheit, Datenschutz und IT-Compliance eng zusammen.

Uni-Siegen CERT

Um Mitglieder und Angehörige (IT-Nutzer) der Universität Siegen möglichst effektiv bei IT-Sicherheitsproblemen unterstützen zu können, sowie eine Durchdringung auch auf operativer E-bene zu erreichen, wird ein Computer Emergency Response Team (CERT) aufgebaut.

Ein Uni-Siegen CERT setzt sich aus folgenden Personen bzw. Funktionsträgerinnen/Funktionsträgern mit den dazugehörigen Aufgabenbereichen zusammen.

a) IT-Sicherheitsteam

Zur Unterstützung der/des IT-Sicherheitsbeauftragten wird ein IT-Sicherheitsteam gemäß Abschnitt 3.1.2 der Ordnung zum Datenschutz und zur IT-Sicherheit aufgestellt. Dieses agiert unabhängig und wird übergreifende Maßnahmen in der Gesamtorganisation koordinieren, in Abstimmung mit der/dem IT-Sicherheitsbeauftragten Kontrollaufgaben durchführen und sie/ihn bei Schulungs- und Sensibilisierungsmaßnahmen unterstützen. Als Teil des CERT verfügt das Team über das entsprechende technische Know-How und hat Kontakt zu den Bereichs-IT-Sicherheitsbeauftragten, um eine angemessene Bearbeitung von Sicherheitsvorfällen zu gewährleisten.

b) Bereichs-IT-Sicherheitsbeauftragte

Jede Fakultät, die Universitätsbibliothek, die Zentrale Universitätsverwaltung und das Zentrum für Informations- und Medientechnologie bestellen je eine Person, die aufgrund ihrer Stellung und beruflichen Erfahrung qualifiziert ist, die Aufgaben der/des Bereichs-IT-Sicherheitsbeauftragten gemäß Abschnitt 3.1.3 der Ordnung zum Datenschutz und zur IT-Sicherheit zu übernehmen. Diese Personen sind Ansprechpartner/innen für die IT-Sicherheit und tragen Sorge für die Umsetzung der im IT-Sicherheitsprozess erarbeiteten Vorgaben in ihrem Bereich. Sie arbeiten eng innerhalb des Uni-Siegen CERT mit dem IT-Sicherheitsteam zusammen.

IT-Servicezentren

Die IT-Grundversorgung an der Universität Siegen wird von drei IT-Servicezentren realisiert.

Das Zentrum für Informations- und Medientechnologie (ZIMT) stellt eine Vielzahl an Diensten und Anwendungen zentral für die Mitarbeiterinnen/Mitarbeiter und Studierenden bereit.

Die Abteilung „IT-Anwendungen in der Verwaltung“ (Dezernat 2) ist für die IT-Versorgung der Zentralen Universitätsverwaltung verantwortlich und stellt die Verwaltungsdienste und anwendungen der gesamten Hochschule zur Verfügung.

Das Sachgebiet "Automatisierte Datenverarbeitung" (im Dezernat 2 der UB) ist für die IT-Versorgung der UB verantwortlich und stellt die Bibliotheksdienste und -anwendungen der gesamten Hochschule zur Verfügung.

Für die technische Durchführung der Maßnahmen im Bereich der IT-Sicherheit und für die Unterstützung der Nutzerinnen/Nutzer in ihrem Zuständigkeitsbereich sind die jeweiligen IT-Servicezentren verantwortlich. Diese arbeiten eng mit der/dem IT-Sicherheitsbeauftragten zusammen.

4. Realisierung des IT-Sicherheitsprozesses

Vorgehen im IT-Sicherheitsprozess

Für die Universität Siegen wird entsprechend den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein allgemeines IT-Sicherheitskonzept erstellt. Aufgrund einer vorausgehenden Strukturanalyse wird der Schutzbedarf der einzelnen IT-Systeme und –Anwendungen festgestellt und ein Basisschutz definiert. Ist der Schutzbedarf einer Komponente höher anzusetzen, so wird eine ergänzende Risikoanalyse für das betreffende System bzw. den betreffenden Dienst durchgeführt und das Schutzniveau entsprechend angepasst.

Folgende IT-Sicherheitsprinzipien sollten bei der Erstellung eines einheitlichen Konzeptes berücksichtigt werden:

- Angehörige werden bezüglich der IT-Sicherheit sensibilisiert,
- IT-Systeme und Daten werden dem Stand der Technik entsprechend vor unberechtigten Zugriffen geschützt,
- Sicherungen der Daten werden durchgeführt, um Benutzerfehlern oder technischem Versagen vorzubeugen,
- IT-Systeme werden in einer sicheren Umgebung betrieben,
- IT-Systeme werden auf dem aktuellen Stand gehalten,
- IT-Systeme werden adäquat vor schädlicher Software (sog. Malware) geschützt,
- die Sicherheitsmaßnahmen werden regelmäßig auf ihre Wirksamkeit hin überprüft und dokumentiert sowie dem Stand der Technik entsprechend angepasst sowie
- IT-Sicherheitsvorfälle werden dokumentiert und kommuniziert.

Aufbauend auf dieser Leitlinie werden in enger Anlehnung an ISO 27001 sowie IT Infrastructure Library (ITIL) allgemeine und detaillierte Richtlinien, in denen sowohl dienste-spezifische als auch zielgruppenbezogene Maßnahmen beschrieben werden, erarbeitet.

Verbesserung der Sicherheit

Das Gesamtkonzept der Informationssicherheit wird regelmäßig auf seine Aktualität, Angemessenheit und Wirksamkeit geprüft.

Die Hochschulleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiterinnen und Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen bzw. Richtlinien und deren Einhaltung wird das angestrebte Sicherheitsniveau gefestigt. Abweichungen werden mit dem Ziel analysiert, das IT-Sicherheitsniveau zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

5. Verstöße gegen die Informationssicherheitsleitlinie

Als Verstöße werden folgende Handlungen verstanden

- das Kompromittieren der Sicherheit von IT-Systemen und Anwendungen,
- der unberechtigte Zugriff auf Informationen und IT-Systeme und
- die unberechtigte Änderung, Nutzung und /oder Veröffentlichung von Informationen.

Verstöße gegen die IT-Sicherheitsleitlinie können nach den geltenden Regelungen und gesetzlichen Bestimmungen geahndet werden.

6. In-Kraft-Treten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung in dem Verkündungsblatt „Amtliche Mitteilungen“ der Universität Siegen“ in Kraft.

Ausgefertigt aufgrund des Beschlusses des Rektorats vom 09. Juni 2011.

Siegen, den 26. Juli 2011

Der Rektor

gez.

(Universitätsprof. Dr. Holger Burckhart)