IT-Sicherheitsordnung
für die Julius-Maximilians-Universität Würzburg

Vom 24. Juli 2006

Die Julius-Maximilians-Universität Würzburg gibt sich die nachfolgende Ordnung zur Regelung des universitätsweiten IT-Sicherheitsprozesses:

Inhaltsübersicht:

Präambel

Funktionierende und sichere IT-Prozesse sind eine zentrale Grundlage für die Leistungsfähigkeit einer Hochschule insbesondere auf den Gebieten Forschung und Lehre. Der Hochschulbetrieb erfordert daher 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 auch für die Universität Würzburg zu, die die Entwicklung und Umsetzung einer einheitlichen hochschulweiten Rahmenordnung der IT-Sicherheit für die Universität erforderlich macht. Hauptziel der Gestaltung von IT-Sicherheit muss es dabei sein, den entsprechenden Rahmen für das Funktionieren von Forschung und Lehre 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 Universität Würzburg gerecht wird. Die Entwicklung und Fortschreibung des IT-

Sicherheitsprozesses muss sich dabei einerseits an den gesetzlich festgelegten Aufgaben der Hochschulen sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren, andererseits ist er nur innerhalb geregelter Verantwor-tungsstrukturen zu erzielen. Es empfiehlt sich daher, diesen IT-Sicherheitsprozess an Prinzipien zu orientieren, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im IT-Grundschutzhandbuch niedergelegt sind.

Diese Ordnung regelt die Zuständigkeiten und die Verantwortung sowie die Zusammenarbeit im universitätsweiten IT-Sicherheitsprozess.

Ziel der IT-Sicherheitsordnung ist es, nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern primär die in der Universität Würzburg verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen zu schützen sowie die Universität Würzburg soweit möglich vor Imageverlust und finanziellen Schäden zu bewahren.

§ 1
Gegenstand der Ordnung

(1) Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines universitätsweiten IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen, eine Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten.

(2) Die Bedingungen, unter denen die IV-Infrastruktur der Universität Würzburg und das damit verbundene Leistungsangebot genutzt werden können, regeln die

- Benutzungsordnung für die Informationsverarbeitungssysteme der Universität Würzburg vom 04. März 2002,
- Benutzungsordnung für das Hochschulnetz der Universität Würzburg vom 04. März 2002, und
- Richtlinien zum Betrieb und Aufbau von WWW-basierten Informationssystemen an der Universität Würzburg vom 25. Juli 2000.

§ 2
Geltungsbereich

Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Organisationseinheiten der Universität Würzburg (Fakultäten, wissenschaftliche Einrichtungen und Betriebseinheiten), auf die gesamte IV-Infrastruktur der Universität, einschließlich der daran betriebenen IT-Systeme sowie die Gesamtheit der Benutzer und Benutzerinnen.

§ 3
Beteiligte am IT-Sicherheitsprozess

Die Gesamtverantwortung für den IT-Sicherheitsprozess liegt bei der Hochschulleitung. Sie bindet bestehende Einrichtungen, insbesondere das Rechenzentrum, in den IT-Sicherheitsprozess ein. Darüber hinaus werden folgende Gremien und Funktionsträger eingesetzt bzw. bestellt:

1. IT-Sicherheitsmanagement-Team (SMT)
2. Operative Gruppe des SMT
3. Dezentrale IT-Sicherheitsbeauftragte

Die Fakultäten sowie die wissenschaftlichen Einrichtung und Betriebseinheiten der Universität Würzburg 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.

§ 4
Einsetzung und Bestellung der Gremien und Funktionsträger

(1) Die Hochschulleitung setzt ein IT-Sicherheitsmanagement-Team (SMT) ein. Die Zusammensetzung des SMT soll - unter Beschränkung der Anzahl der Mitglieder auf das erforderliche Maß - sowohl die unterschiedlichen Aufgabenbereiche der Universität Würzburg widerspiegeln als auch die unterschiedlichen, für die Universität relevanten Aspekte der IT-Sicherheit berücksichtigen. Ständige Mitglieder des SMT sind:

- der Vizepräsident oder die Vizepräsidentin, in dessen oder deren Geschäftsbereich das IT-Sicherheitsmanagement fällt,
- die Kanzlerin,
- ein Vertreter oder eine Vertreterin aus dem Kreis der Hochschullehrer und Hochschullehrerinnen als Bindeglied zwischen IT-Dienstleistern und Wissenschaftlern und Wissenschaftlerinnen,
- ein Vertreter oder eine Vertreterin der dezentralen IT-Sicherheitsbeauftragten,
- ein Vertreter oder eine Vertreterin des Rechenzentrums, in der Regel dessen Leiter oder Leiterin,
- ein Vertreter oder eine Vertreterin der Universitätsbibliothek, in der Regel deren Leiter oder Leiterin.

Mit Ausnahme des Vizepräsident oder die Vizepräsidentin, in dessen oder deren Geschäftsbereich das IT-Sicherheitsmanagement fällt, und der Kanzlerin werden die ständigen Mitglieder vom Präsidenten bestellt; weitere sachverständige Mitglieder werden vom Präsidenten im Benehmen mit der Ständigen Kommission für Angelegenheiten des Rechenzentrums bestellt. Die Bestellung kann befristet werden.

(2) Den Vorsitz im SMT hat der Vizepräsident oder die Vizepräsidentin. Die Stellvertretung obliegt der Kanzlerin.

(3) Das SMT setzt eine Arbeitsgruppe ein (Operative Gruppe), die das SMT im operativen Geschäft unterstützt, deren Mitglieder aus dem Kreis

- der Mitglieder des SMT und
- der IT-Sicherheitsspezialisten des Rechenzentrums

von dem/der Vorsitzenden des SMT im Benehmen mit den ständigen Mitgliedern bestellt werden.

(4) Das SMT und die Operative Gruppe können bei Bedarf den Rat von Experten und Expertinnen einholen (z.B. von Juristen und Juristinnen, Spezialisten oder Spezialistinnen für Teilbereiche der IT-Sicherheit).

(5) Jede Fakultät und jede wissenschaftliche Einrichtung und Betriebseinheit der Universität Würzburg hat eine(n) dezentrale(n) IT-Sicherheitsbeauftragte(n) und eine Stellvertretung zu bestellen. Ein(e) dezentrale(r) IT-Sicherheitsbeauftragte(r) kann für mehrere Fakultäten oder wissenschaftliche Einrichtungen und Betriebseinheiten zuständig sein. Jede Fakultät und jede wissenschaftliche Einrichtung und Betriebseinheit trägt Sorge dafür, dass durch die Bestellung(en) alle IT-Systeme im Verantwortungsbereich sowie die für den Betrieb vor Ort verantwortlichen Personen einem/einer IT-Sicherheits-beauftragten zugeordnet werden.

(6) Bei der Bestellung der im IT-Sicherheitsprozess aktiven Personen soll die erforderliche personelle Kontinuität berücksichtigt werden. Deshalb sollen IT-Sicherheitsbeauftragte über langfristige Verträge verfügen oder möglichst zum hauptberuflichen Personal der Universität Würzburg gehören.

(7) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leitung der Organisationseinheiten 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 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 dokumentiert sicherheitsrelevante Vorfälle und erstellt jährlich einen IT-Sicherheitsbericht.

(4) Die Operative Gruppe unterstützt das SMT bei der Wahrnehmung seiner Aufgabe, das beschlossene IT-Sicherheitskonzept umzusetzen. Bei ihrer Einsetzung werden die Aufgaben und Zuständigkeiten im Einzelnen festgelegt. Außerdem ist sie für die Organisation von Schulungen und Weiterbildungsmaßnahmen der dezentralen IT-Sicherheitsbeauftragten zuständig und unterstützt diese bei der Konzeptumsetzung.

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

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

(7) Die am IT-Sicherheitsprozess Beteiligten haben in allen Belangen der IT-Sicherheit zusammenzuarbeiten, sich die dazu erforderlichen Informationen bereitzustellen und die Kommunikations- und Entscheidungswege sowohl untereinander als auch in Beziehung zu Dritten festzulegen. In Krisensituationen haben alle Beteiligten der Beseitigung der IT-Sicherheitsrisiken Vorrang vor anderen Dienstaufgaben einzuräumen.

§ 6
Umsetzung des IT-Sicherheitsprozesses

(1) Die Umsetzung des IT-Sicherheitsprozesses, der nach den festzulegenden Prioritäten technische und organisatorische Maßnahmen sowohl präventiver als auch reaktiver Art sowie Maßnahmen zur schnellen Krisenintervention umfassen muss, wird durch das SMT initiiert, gesteuert und kontrolliert.

(2) Die zu erarbeitenden Notfallpläne, die Handlungsanweisungen und Verhaltensregeln für bestimmte Gefahrensituationen und Schadensereignisse zu beinhalten haben, sollen das Ziel verfolgen, Gefahren soweit möglich abzuwenden sowie eine möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen zu ermöglichen.

(3) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Zuständigkeitsbereich verantwortlich. Mit der Bestellung kommen ihnen die zur Wahrnehmung ihrer Aufgaben erforderlichen Befugnisse in ihrem Zuständigkeitsbereich zu. Sie informieren regelmäßig sowohl die Leitung ihrer Organisationseinheit als auch das SMT über den Stand der Umsetzung und über aktuelle Problemfälle.

(4) Das SMT beruft einen Arbeitskreis aus dem Kreis der dezentralen IT-Sicherheitsbeauftragten, dem die Aufgabe zukommt, aufgrund der gemachten Erfahrungen gemeinsame Empfehlungen für die hochschulweite Umsetzung des IT-Sicherheitsprozesses dem SMT zu geben.

(5) Alle Mitglieder und Angehörigen der Universität Würzburg sowie Benutzer der IT-Infrastruktur sind zur Meldung sicherheitsrelevanter Ereignisse an die dezentralen IT-Sicherheitsbeauftragten verpflichtet.

(6) Richtlinien und Notfallpläne sind ortsüblich bekannt zu machen und verbindlich für die in § 2 beschriebenen Bereiche.

§ 7
Krisenintervention

(1) Bei Gefahr im Verzuge veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige Stilllegung betroffener IT-Systeme in ihrem Zuständigkeitsbereich, wenn zu befürchten ist, dass sich ein voraussichtlich gravierender Schaden nicht anders abwenden lässt. Das SMT ist über diese vorläufige Maßnahme, sobald es die Situation zulässt, unverzüglich zu informieren.

(2) Soweit das Rechenzentrum Gefahr im Verzuge feststellt, kann es Netzanschlüsse (ggf. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend oder auf längere Dauer sperren, wenn zu befürchten ist, dass sich ein voraussichtlich gravierender Schaden für die IT-Infrastruktur oder sonstige erhebliche Verletzungen von Interessen der Universität Würzburg oder Rechten Dritter in Teilen oder insgesamt nicht anders abwenden lässt. Der zuständige dezentrale IT-Sicherheitsbeauftragte sowie das SMT sind, sobald es die Situation zulässt, unverzüglich zu informieren.

(3) Die Wiederinbetriebnahme stillgelegter oder gesperrter IT-Systeme 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 Organisationseinheit der Universität Würzburg sind von der betreffenden Einheit zu erbringen. Darunter fallen auch die Schulungskosten für den/die dezentralen IT-Sicherheitsbeauftragten sowie für ihre Benutzer und Benutzerinnen.

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

§ 9
In-Kraft-Treten

Diese Ordnung tritt nach ihrer Beschlussfassung im Senat am Tag nach ihrer Bekanntmachung in Kraft.

Ausgefertigt aufgrund des Beschlusses des Senats der Universität Würzburg vom 24. Mai 2006.

Würzburg, den 24. Juli 2006

Der Präsident:

_____

Prof. Dr. A. Haase

Die IT-Sicherheitsordnung für die Julius-Maximilians-Universität Würzburg wurde am 26. Juli 2006 in der Universität niedergelegt. Die Niederlegung wurde am 27. Juli 2006 durch Anschlag in der Universität bekannt gegeben. Tag der Bekanntgabe ist daher der 27. Juli 2006.

Würzburg, den 28. Juli 2006

Der Präsident:

_____

Prof. Dr. A. Haase