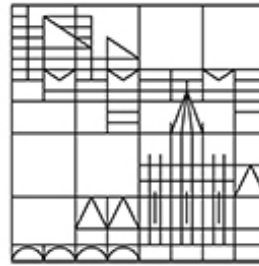


Universität
Konstanz



Amtliche Bekanntmachung der Universität Konstanz

Nr. 10/2012

**Leitlinie zur Informationssicherheit der
Universität Konstanz**

Vom 6. März 2012

Leitlinie zur Informationssicherheit der Universität Konstanz

1. Motivation

Die Universität Konstanz steht für Exzellenz in Forschung und Lehre und genießt weltweit einen sehr guten Ruf. Wissenschaftlern und Dozenten stellt die Universität eine Plattform zur Verfügung, die zu herausragenden Leistungen motiviert. Das Ziel der Informationssicherheit ist die Bereitstellung einer IT-Infrastruktur, die eine ausgezeichnete Betriebsstabilität und Verfügbarkeit aufweist sowie einen vertrauenswürdigen Rahmen für Kooperationen mit anderen Forschungseinrichtungen, Unternehmen und Geschäftspartnern bietet. Die Universität strebt eine zielgerichtete Auswahl geeigneter Maßnahmen an, um den hohen Anforderungen an die Funktionsfähigkeit und Sicherheit der Informationen, Dienste sowie Server und Netze gerecht zu werden. Die gezielte Begegnung der stetig steigenden Gefahren der IT-Landschaft minimiert die Angriffsfläche der Angreifer auf das heterogene Universitätsnetz. Durch die zweckmäßige Auswahl der Sicherheitsmaßnahmen ist die Universität in der Lage das Risiko für den Ausfall von Diensten oder Servern beziehungsweise den Zusammenbruch des gesamten Netzes zu reduzieren und so die Lehr- und Forschungstätigkeit sowie die Verwaltung der Universität aufrecht zu erhalten. Finanzielle Schäden verhindert die Universität durch einen Schutz gegen das Ausspähen oder Manipulieren von sensiblen Forschungsdaten und -ergebnissen. Sicherheitsvorfälle, wie beispielsweise Angriffe auf Server und Ausspähen vertraulicher Informationen, sollen frühzeitig erkannt und geeignet behandelt werden, um das Image der Universität in der öffentlichen Wahrnehmung zu schützen.

Die Universitätsleitung ist der Überzeugung, dass ein kompetenter Umgang mit den Gefahren und die Etablierung und Aufrechterhaltung eines kontinuierlichen Informationssicherheits-Management-prozesses wichtig für eine zukunftsfähige Universität ist.

2. Sicherheitsziele

Die Sicherheitsziele sind:

- Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen und Informationen,
- Schutz des Netzwerks, der Rechnersysteme und Informationen (Hardware und Software) gegen Missbrauch von innen und außen,
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen des Datenschutzes,
- Sicherstellung eines reibungslosen Lehr-, Forschungs- und Verwaltungsbetriebes sowie
- die Gewährleistung des guten Rufes der Universität in der Öffentlichkeit.

Zur Umsetzung dieser Sicherheitsziele, beschließt das Rektorat diese Leitlinie und unterstützt in vollem Maß die daraus abgeleiteten Sicherheitskonzepte und -maßnahmen.

3. Verantwortlichkeiten

Folgende Verantwortlichkeiten werden definiert:

- Gesamtverantwortung

- Zentrales Informationssicherheits-Management
- Umsetzung von Sicherheitsmaßnahmen
- Rechtsberatung in Datenschutzfragen

Gesamtverantwortung

Die Gesamtverantwortung für die Informationssicherheit liegt beim Rektorat der Universität Konstanz.

Zentrales Informationssicherheits-Management

Das zentrale Informationssicherheits-Management erarbeitet Sicherheitsrichtlinien und koordiniert den Informationssicherheits-Managementprozess innerhalb der Universität und kann die Umsetzung von notwendigen Sicherheitsmaßnahmen durch die dezentralen IT-Sicherheitsbeauftragten anweisen. Des Weiteren unterstützt es die dezentralen IT-Sicherheitsbeauftragten mit Hinweisen und Informationen. Außerdem berichtet das zentrale Informationssicherheits-Management in regelmäßigen Abständen über KIM an die Universitätsleitung über Aktivitäten.

Umsetzung von Sicherheitsmaßnahmen

Die Leiter der einzelnen Organisationseinheiten (z.B. der zentralen Bereiche wie Verwaltung, Bibliothek, Rechenzentrum, etc.) und der zentralen Einrichtungen in der Forschung und Lehre (z.B. Arbeitsgruppen, Fachbereiche, Sonderforschungsbereiche etc.) sind für die Sicherheit der dort betriebenen IT-Systeme, Netze sowie die gespeicherten Daten verantwortlich im Rahmen ihrer Entscheidungsbefugnisse und sorgen für die Umsetzung der notwendigen Sicherheitsmaßnahmen in der jeweiligen Organisationseinheit.

Jeder Endbenutzer ist verantwortlich für den gewissenhaften Umgang mit den, ihm zugänglichen, Informationen und ist verpflichtet die jeweils für seinen Bereich gültigen (Sicherheits-)Richtlinien umzusetzen.

Rechtsberatung in Datenschutzfragen

Der Justitiar berät und unterstützt das zentrale Informationssicherheits-Management in juristischen Fragen des Datenschutzes.

Zur Wahrnehmung der Verantwortlichkeiten wird folgende Organisationsstruktur eingerichtet.

4. Organisationsstruktur

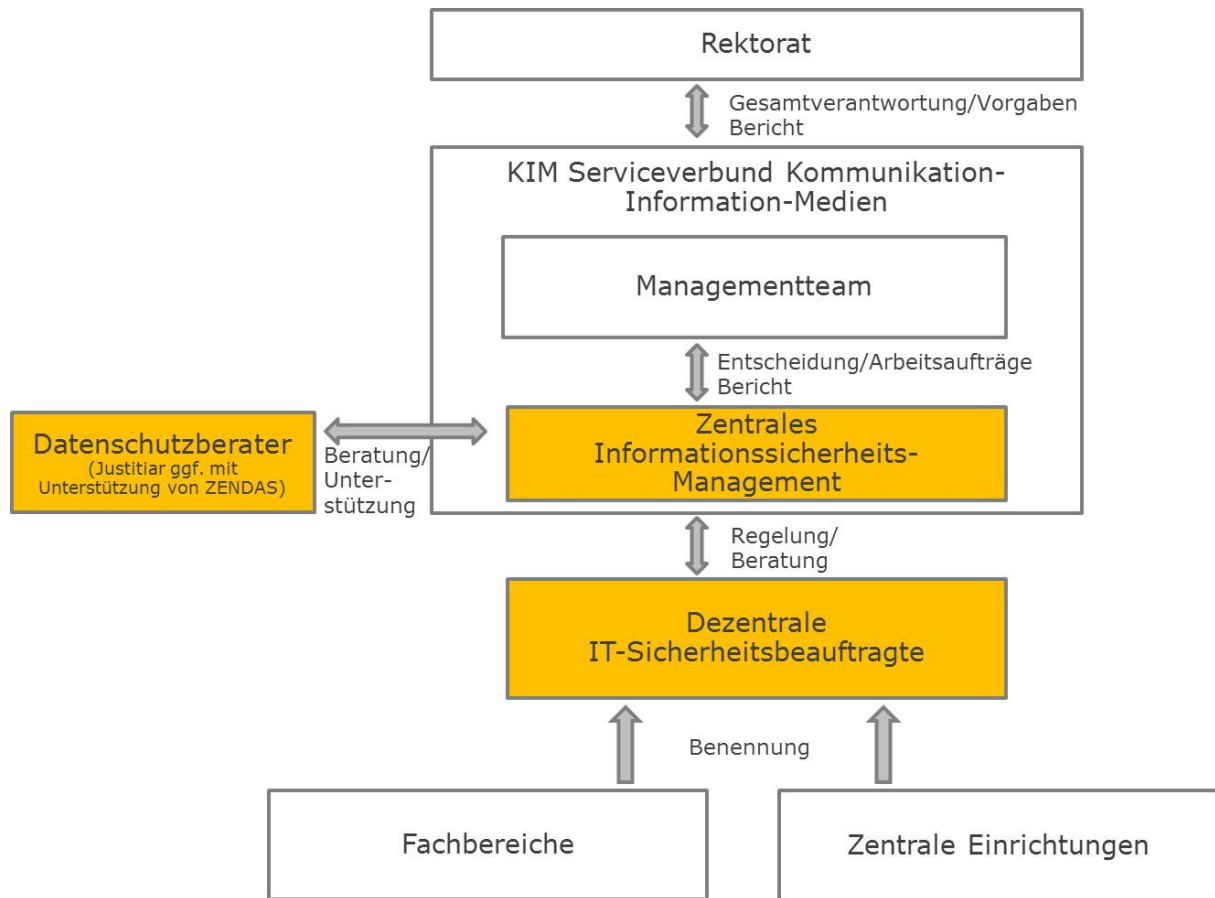


Abb.: 1 Organisationsstruktur des Informationssicherheits-Managements

Bei einer großen Organisation wie der Universität Konstanz ist ein Informationssicherheitskonzept nur in einer mehrstufigen Organisationsstruktur umzusetzen. Folgende Organisationsstruktur wird eingerichtet:

- ein zentrales Informationssicherheits-Management,
- die dezentralen Sicherheitsbeauftragten sowie
- der Datenschutzberater (vgl. Abb.: 1).

Zentrales Informationssicherheits-Management

Das zentrale Informationssicherheits-Management wird vom Serviceverbund Kommunikation-Information-Medien (KIM) gestellt. Das zentrale Informationssicherheits-Management organisiert regelmäßig Arbeitstreffen mit den dezentralen IT-Sicherheitsbeauftragten und bei Bedarf werden adhoc Arbeitsgruppen gebildet, die bestimmte Inhalte übergreifend erarbeiten.

Dezentrale IT-Sicherheitsbeauftragte

Jede zentrale Einrichtung (z.B. Verwaltung, Bibliothek, Rechenzentrum, etc.) benennt einen Ansprechpartner als dezentralen Sicherheitsbeauftragten. In den Sektionen benennt jeder Fachbereich einen Ansprechpartner, der für die IT-Sicherheitsbelange zuständig ist. Es ist möglich, dass mehrere Fachbereiche dieselbe Person benennen. Es ist auch möglich, dass ein Fachbereich mehrere dezentrale Sicherheitsbeauftragte benennt,

wenn die notwendigen IT-Kompetenzen vorhanden sind. Diese Aufgabe kann z.B. an die zuständigen Netzadministratoren delegiert werden. Von welchen Einheiten dezentrale IT-Sicherheitsbeauftragte benannt werden müssen, wird vom zentralen Informationssicherheits-Management festgelegt. Diesbezügliche Vereinbarungen müssen schriftlich fixiert und dem zentralen Informationssicherheits-Management bekannt gegeben werden.

Datenschutzberater

Die juristische Datenschutzberatung wird vom Justitiar, gegebenenfalls mit Unterstützung von ZENDAS, erfüllt.

5. Maßnahmen der Gefahrenabwehr

Um die Sicherheitsziele zu erreichen, etabliert die Universität einen zentralen Informationssicherheits-Managementprozess, der sich an dem in Deutschland für öffentliche Einrichtungen etablierten Standard des IT-Grundschutzes orientiert und folgende Phasen umfasst:

- Initiierung des Sicherheitsprozesses (u.a. Verantwortung der Leitungsebene, Konzeption u. Planung)
- Erstellung einer Sicherheitskonzeption (Schutzbedarfsfeststellung, Sicherheitscheck, Maßnahmenempfehlung)
- Umsetzung der Sicherheitskonzeption
- Aufrechthaltung und Verbesserung

Konkrete Maßnahmen technischer, physischer und organisatorischer Art werden auf Basis von Sicherheitsanalysen unter Beachtung von Kosten- und Wirksamkeitsaspekten empfohlen und umgesetzt. Technischen Maßnahmen sind bspw. der Einsatz von Firewalls, Antiviren- und Antispam-Programmen. Zu den physischen Maßnahmen gehört bspw. der Einsatz von Zutrittsbeschränkungen zu Räumen mit erhöhtem Schutzbedarf (z.B. Serverräume). Organisatorische Maßnahmen umfassen unter anderem die Erstellung von Satzungen, Ordnungen und sonstigen Richtlinien für Informationssicherheit. Weitere Maßnahmen sind die Sensibilisierung der Beschäftigten und Studierenden für die Risiken sowie die Durchführung von Schulungen.

6. Inkrafttreten und Geltungsbereich

Die Leitlinie wurde vom Senat sowie vom Rektorat der Universität Konstanz für die gesamte Organisation verabschiedet und tritt zum 22.02.2012 in Kraft. Fachspezifische Richtlinien (z.B. zur IT-Nutzung) werden in separaten Dokumenten zur Verfügung gestellt.

Konstanz, 6. März 2012

gez.

Prof. Dr. Ulrich Rüdiger - Rektor -