

# Mitteilungen der Bauhaus-Universität Weimar

<input checked="" type="checkbox"/> Der Rektor Bauhaus-Universität	IT-Sicherheitsordnung für die Hochschule für Musik FRANZ LISZT Weimar und die Bauhaus-Universität Weimar		Ausgabe 10/2005
<input checked="" type="checkbox"/> Der Rektor Hochschule für Musik FRANZ LISZT	erarb. Dez./Einheit SCC	Telefon 2400	Datum 4. Juli 2005

## Präambel

Funktionierende und sichere IT-Prozesse sind eine maßgebliche Voraussetzung für die Leistungsfähigkeit einer Hochschule auf den Gebieten Lehre und Forschung. Der Hochschulbetrieb erfordert in zunehmendem 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 in Hochschulen zu, die die Entwicklung und Umsetzung einer einheitlichen hochschulübergreifenden Rahmenrichtlinie der IT-Sicherheit erforderlich macht. Hauptziel der IT-Sicherheitspolitik muss es sein, den entsprechenden Rahmen für das Funktionieren von Lehre und Forschung 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 Hochschulen gerecht wird.

Diese Ordnung regelt die Zuständigkeiten und die Verantwortung sowie die Zusammenarbeit im hochschulweiten IT-Sicherheitsprozess. Ziel der IT-Sicherheitsordnung ist es, nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern auch die Hochschulen soweit möglich vor Imageverlust und finanziellen Schäden zu bewahren. Die Entwicklung und Fortschreibung der Rahmenrichtlinie der IT-Sicherheit 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) im IT-Grundschutzhandbuch niedergelegt sind.

## § 1 - Gegenstand der Ordnung

Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines hochschulübergreifenden IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen, eine Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten. Diese Ordnung wird ergänzt durch die Ordnung für die Nutzung der IV-Infrastruktur der Bauhaus-Universität Weimar.

## § 2 - Geltungsbereich

- (1) Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Einrichtungen der Bauhaus-Universität Weimar und der Hochschule für Musik Franz Liszt Weimar (Fachbereiche, wissenschaftliche und künstlerische Einrichtungen, zentrale Einrichtungen und sonstige Einrichtungen), auf die gesamte IT-Infrastruktur der Bauhaus-Universität und der Hochschule für Musik, einschließlich aller betriebenen IT-Systeme.
- (2) Die Festlegungen dieser Ordnung und der hieraus entstehenden Rahmenrichtlinien sind bei Vereinbarungen und Verträgen mit An-Instituten und außeruniversitären Einrichtungen, die direkt an das Hochschulnetz angeschlossen sind oder über dieses die Mitnutzer des Deutsche Forschungsnetzes (DFN) sind, zu beachten.

### § 3 - Beteiligte am IT-Sicherheitsprozess

Die Hauptverantwortung für den IT-Sicherheitsprozess liegt bei den Hochschulleitungen. Sie setzen daher gemeinsam folgende Gremien und Funktionsträger ein:

- IT-Sicherheits-Management-Team (SMT)
- Operative Gruppe des SMT
- Dezentrale IT-Sicherheitsbeauftragte
- Servicezentrum für Computersysteme und -kommunikation (SCC)
- Einrichtungen der Hochschulen

### § 4 - Einsetzung der Beteiligten

- (1) Die Hochschulleitungen setzen gemeinsam ein IT-Sicherheits-Management-Team (SMT) ein. Ständige Mitglieder des SMT sind:
  - ein Vertreter jeder der beiden Hochschulleitungen,
  - die Datenschutzbeauftragten der Hochschulen,
  - der Justiziar der Bauhaus-Universität,
  - der zentrale IT-Sicherheitsbeauftragte der Bauhaus-Universität,
  - der Leiter des SCC.
- (2) Das SMT setzt eine Arbeitsgruppe ein, die das SMT im operativen Geschäft unterstützt (Operative Gruppe). Ständige Mitglieder sind:
  - der zentrale IT-Sicherheitsbeauftragte
  - ein Vertreter der dezentralen IT-Sicherheitsbeauftragten,
  - ein Vertreter der dezentralen Administratoren (DV-Org).
- (3) Das SMT und die Operative Gruppe sollen sich bei Bedarf den Rat von Experten einholen (z. B. Spezialisten für Teilbereiche der IT-Sicherheit).
- (4) Nach Vorgabe des SMT sind dezentrale IT-Sicherheitsbeauftragte und Stellvertreter zu benennen. Durch die Benennung müssen alle IT-Systeme im Geltungsbereich sowie die für den Betrieb vor Ort verantwortlichen Personen einem IT-Sicherheitsbeauftragten zugeordnet sein.
- (5) Bei der Bestellung/Benennung der im IT-Sicherheitsprozess aktiven Personen soll die erforderliche personelle Kontinuität berücksichtigt werden. Deshalb sollen die IT-Sicherheitsbeauftragten über langfristige Verträge verfügen oder möglichst zum hauptamtlichen Personal der jeweiligen Hochschule gehören.
- (6) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leitung der Einrichtungen nicht von ihrer Gesamtverantwortung für die IT-Sicherheit in ihrem Zuständigkeitsbereich.

### § 5 - Aufgaben der Beteiligten

- (1) Das SMT arbeitet strategisch und ist für die Erstellung der Rahmenrichtlinien, Fortschreibung, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.
- (2) Die Operative Gruppe unterstützt das SMT bei der Wahrnehmung seiner Aufgaben, die beschlossenen IT-Sicherheitsrahmenrichtlinien umzusetzen und gibt die hochschulinternen technischen Standards zur IT-Sicherheit vor. Außerdem ist sie für die Schulung und Weiterbildung der dezentralen IT-Sicherheitsbeauftragten zuständig und unterstützt diese bei der Umsetzung der Rahmenrichtlinien.
- (3) Das SMT/Operative Gruppe dokumentieren sicherheitsrelevante Vorfälle und erstellen jährlich einen IT-Sicherheitsbericht.
- (4) Die IT-Sicherheitsbeauftragten sind für die Umsetzung aller mit dem SMT abgestimmten Sicherheitsbelange bei den IT-Systemen und -Anwendungen sowie den Mitarbeitern in ihren Bereichen verantwortlich. Sie sind verpflichtet, sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf einem aktuellen Stand zu halten.
- (5) Das SCC ist für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit verantwortlich. Es arbeitet eng mit der Operativen Gruppe des SMT zusammen.

- (6) Die Einrichtungen der Hochschulen 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.
- (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. Hierbei ist insbesondere der Aspekt der in Krisensituationen gebotenen Eile zu berücksichtigen.

## **§ 6 - Umsetzung des IT-Sicherheitsprozesses**

- (1) Das SMT initiiert, steuert und kontrolliert die Umsetzung des IT-Sicherheitsprozesses, der nach festzulegenden Prioritäten technische und organisatorische Maßnahmen sowohl präventiver als auch reaktiver Art sowie Maßnahmen zur schnellen Krisenintervention umfassen muss.
- (2) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Zuständigkeitsbereich verantwortlich. Dafür müssen sie vom SMT und der Leitung der jeweiligen Einrichtung mit entsprechenden Kompetenzen ausgestattet werden. Sie informieren regelmäßig sowohl die Leitung ihrer Einrichtung als auch das SMT/Operative Gruppe über den Stand der Umsetzung und über aktuelle Problemfälle.
- (3) Das SMT setzt den Arbeitskreis DV-Org ein, der primär als Basis dienen soll, um die Umsetzung des IT-Sicherheitsprozesses hochschulweit abzustimmen und Erfahrungen auszutauschen.

## **§ 7 - Notfallvorsorge**

- (1) Für akute Störfälle sowie für eine möglichst schnelle Wiederherstellung der Verfügbarkeit der IT-Ressourcen nach Eintritt von Schadensereignissen sind Notfallpläne für wichtige Dienste in allen Einrichtungen der Hochschulen, insbesondere für zentrale Dienste im SCC zu erarbeiten, durch Notfallübungen zu überprüfen und regelmäßig fortzuschreiben. Die Einzelheiten über den Erlass und die Umsetzung der Notfallpläne regelt das SMT.
- (2) Bei Gefahr im Verzuge veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige vorübergehende Stilllegung betroffener IT-Systeme in ihrem Zuständigkeitsbereich, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden nicht anders abzuwenden ist. Die Operative Gruppe ist unverzüglich zu informieren.
- (3) Die Wiederinbetriebnahme erfolgt erst nach der Durchführung hinreichender Sicherheitsmaßnahmen in Abstimmung mit der Operativen Gruppe.

## **§ 8 - Finanzierung**

- (1) Die personellen und finanziellen Ressourcen für alle erforderlichen IT-Sicherheitsmaßnahmen in einer Einrichtung der Bauhaus-Universität und der Hochschule für Musik 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 Ansätzen zu finanzieren.

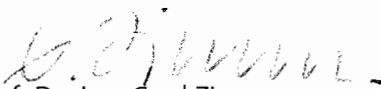
## § 9 - Gleichstellungsklausel


Status- und Funktionsbezeichnungen nach dieser Ordnung gelten gleichermaßen in der weiblichen wie in der männlichen Form.

## § 10 - In-Kraft-Treten

Diese Ordnung tritt nach ihrer Bestätigung im jeweiligen Senat der Hochschulen am Tag nach ihrer Bekanntmachung in Kraft.

Weimar, 4. Juli 2005

  
Prof. Dr.-Ing. Gerd Zimmermann  
Rektor der Bauhaus-Universität

  
Prof. Rolf-Dieter Arens  
Rektor der Hochschule  
für Musik FRANZ LISZT