Gemeinsame IT-Sicherheits-Leitlinie der Bauhaus-Universität Weimar sowie der Hochschule für Musik Franz Liszt Weimar

Gemäß § 29 Abs. 1 S. 2 1. HS Thüringer Hochschulgesetz (ThürHG) vom 10. Mai 2018 (GVBl. S. 149) geben sich die Bauhaus–Universität Weimar (BUW) sowie die Hochschule für Musik Franz Liszt Weimar (HfM) die folgende Gemeinsame IT-Sicherheits-Leitlinie.

Das Präsidium der BUW hat die Leitlinie am 30. Mai 2018 beschlossen.

Das Präsidium der HfM hat die Leitlinie am 19. Juni 2018 beschlossen, der Senat der HfM hat sie am 25. Juni 2018 zustimmend zur Kenntnis genommen.

Präambel

Die Leistungsfähigkeit einer Hochschule in Forschung, Lehre und Verwaltung hängt maßgeblich von der Qualität und Sicherheit der eingesetzten Informationstechnologie (IT) ab. Die heterogene IT-Infrastruktur, die hohe Zahl vernetzter Systeme, die Komplexität der vielfältigen IT-Services und die verteilte Verantwortlichkeit erfordern die Etablierung und Fortschreibung eines hochschulweiten und kontinuierlichen IT-Sicherheitsprozesses. Vertraulichkeit, Verfügbarkeit und Integrität von Informationen, Services und IT-Systemen sind angemessen und risikogerecht zu gewährleisten. Der Informationssicherheit kommt daher eine grundsätzliche, strategische Bedeutung zu.

Diese Leitlinie regelt die Zuständigkeiten und die Verantwortlichkeiten an den Weimarer Hochschulen sowie die Zusammenarbeit im hochschulweiten und hochschulübergreifenden IT-Sicherheitsprozess.
Ein angemessenes IT-Sicherheitsniveau soll unter Wahrung der akademischen Freiheit mögliche Schäden bereits im Ansatz vermeiden und die Hochschulen bei ihren Aufgaben unterstützen.

§ 1 - Gegenstand der Leitlinie

Gegenstand dieser Leitlinie ist die Festlegung der zur Realisierung eines hochschulübergreifenden IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen, eine Aufgabenzuordnung sowie die Festlegung der Zusammenarbeit der Beteiligten.

§ 2 - Geltungsbereich

(1) Der Geltungsbereich dieser Leitlinie erstreckt sich auf alle Einrichtungen der BUW und der HfM sowie alle Einrichtungen, die durch die BUW mit IT versorgt werden, auf die gesamte IT-Infrastruktur der BUW und der HfM, einschließlich aller betriebenen IT-Systeme.

(2) Die Festlegungen dieser Leitlinie sind bei Vereinbarungen und Verträgen mit An-Instituten und außeruniversitären Einrichtungen, die direkt an das Hochschulnetz angeschlossen sind oder über dieses Mitnutzer des Deutschen Forschungsnetzes (DFN) sind, zu beachten.

§ 3 - Beteiligte am IT-Sicherheitsprozess

Die Hauptverantwortung für den IT-Sicherheitsprozess liegt bei den jeweiligen Hochschulleitungen. Spezielle Aufgaben tragen:

- das IT-Sicherheits-Management-Team (SMT),
- die Operative Gruppe des SMT,
- die dezentralen IT-Sicherheitsbeauftragten,
- das Servicezentrum für Computersysteme und -kommunikation (SCC),
- die Einrichtungen der Hochschulen.

§ 4 - Einsetzung der Beteiligten

(1) Die Hochschulleitungen setzen gemeinsam ein IT-Sicherheits-Management-Team (SMT) ein. Ständige Mitglieder des SMT sind:

- je ein Vertreter der beiden Hochschulleitungen,
- die Datenschutzbeauftragten der beiden Hochschulen,
- jeweils ein Justiziar der beiden Hochschulen,
- der zentrale IT-Sicherheitsbeauftragte der BUW,
- der Leiter des SCC.

(2) Das SMT setzt eine Arbeitsgruppe ein, die das SMT im operativen Geschäft unterstützt (Operative Gruppe). Mitglieder sind:

- der zentrale IT-Sicherheitsbeauftragte der BUW,
- Vertreter der dezentralen IT-Sicherheitsbeauftragten,
- 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 ist die erforderliche personelle Kontinuität zu berücksichtigen. 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 Fortschreibung, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.

(2) Die Operative Gruppe unterstützt das SMT bei der Wahrnehmung seiner Aufgaben, gibt die hochschulinternen technischen Standards zur IT-Sicherheit vor und bearbeitet und dokumentiert die IT-Sicherheitsrelevanten Vorfälle in ihrem Bereich.

(3) Der durch den zentralen IT-Sicherheitsbeauftragten jährlich zu erstellende IT-Sicherheitsbericht wird durch das SMT bestätigt.

(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 BUW und der HfM 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

Alle Personen-, Status- und Funktionsbezeichnungen in dieser Leitlinie gelten gleichermaßen für Frauen, Männer und Menschen, die sich keinem dieser Geschlechter zuordnen.

§ 10 – In-Kraft-Treten

(1) Diese Leitlinie tritt am ersten Tag des auf ihre Bekanntmachung im Verkündungsblatt der jeweiligen Hochschule folgenden Monats für die jeweilige Hochschule in Kraft.

(2) Gleichzeitig tritt die IT-Sicherheitsordnung für die Hochschule für Musik Franz Liszt Weimar und die Bauhaus Universität Weimar vom 04. Juli 2005 (BUW: MdU 10/2005, S. 62, HfM: VBl. 01/2006, S. 5) für die jeweilige Hochschule außer Kraft.

Weimar, den 25. Juni 2018

Prof. Dr. Christoph Stölzl
Präsident