IT-Sicherheitsleitlinie
der
Hochschule für Musik „Hanns Eisler“

Vorwort

Diese Leitlinie regelt die besonderen Sicherheitsbedürfnisse und -anforderungen der **Hochschule für Musik „Hanns Eisler“** (im Folgenden Hochschule genannt) sowie die Umsetzung beim Betrieb von IT-gestützten Verfahren bzw. den in der Hochschule eingesetzten IT-Systemen.

Die hier vorliegende ”IT-Sicherheitsleitlinie” ist Bestandteil des Risikomanagements der Hochschule.

Die Hochschulleitung verabschiedet hiermit folgende IT-Sicherheitsleitlinie als Bestandteil ihrer Strategie.

Geltungsbereich

Der Geltungsbereich erstreckt sich auf die Hochschule als Teil des IT-Verbundes der Berliner Kunsthochschulen, betreut vom ServiceCenter IT, einer gemeinsamen Einrichtung der Hochschule für Musik "Hanns Eisler", der Hochschule für Schauspielkunst "Ernst Busch" und der Kunsthochschule Berlin-Weißensee. Diese Leitlinie ist bindend für alle natürlichen und juristischen Personen, welche die IT-Infrastruktur des Hochschulverbundes an der Hochschule nutzen.

I. Stellenwert der Informationsverarbeitung

Informationsverarbeitung spielt eine Schlüsselrolle bei der Aufgabenerfüllung. Die Organisation und Aufrechterhaltung des Lehrbetriebs und der Verwaltung ist in hohem Maße von funktionierender Informationstechnologie abhängig. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben - speziell in den Bereichen Studien- und Prüfungsverwaltung, Haushalt und Personal - werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf der Hochschulbetrieb nicht zusammenbrechen.

II. Übergreifende Ziele

- Festlegung des erforderlichen Sicherheitsniveaus der IT-Systeme der Hochschule anhand des BSI IT-Grundschutzhandbuchs
- Definition der sich daraus ableitenden Schutzziele und Schutzmaßnahmen
- Risikoanalyse
- Ableitung des daraus resultierenden Handlungsbedarfs für die unterschiedlichen Rollen im IT-Sicherheitskreislauf
- Definition von einheitlichen und nachvollziehbaren Prüfkriterien beim Betrieb von IT-Systemen innerhalb der Hochschule
- Beitrag zur Vereinheitlichung des Risikomanagements in der Hochschule bezüglich der Beurteilung des IT-Betriebsrisikos
- Förderung des IT-Sicherheitsbewusstseins in der Hochschule

- Bestandteil der umfassenden Dokumentation des Risikomanagements für interne und externe Stellen (Rechnungshof, etc.)
- Erlass von Nutzungsordnungen für die Anwenderinnen und Anwender für den Betrieb von IT Systemen

Die Daten und IT-Systeme werden in allen technikabhängigen Bereichen der Verwaltung und Lehre in ihrer *Verfügbarkeit* so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (*Integrität*). Die Anforderungen an *Vertraulichkeit* haben ein normales, an Gesetzeskonformität orientiertes Niveau.

IT-Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen. Schadensfälle mit hohen finanziellen Auswirkungen oder Schadensfälle die den Ruf der Hochschule beschädigen können, müssen verhindert werden.

Alle Beschäftigten der Hochschule sind verpflichtet die einschlägigen Gesetze und vertraglichen Regelungen einzuhalten. Negative finanzielle und immaterielle Folgen für die Hochschule sowie für die Beschäftigten durch Rechtsverstöße sind zu vermeiden.

Alle Beschäftigten und die Hochschulleitung sind sich ihrer Verantwortung beim Umgang mit der IT bewusst und unterstützen die IT-Sicherheitsstrategie nach besten Kräften.

1. Schutzziele

Alle sensiblen Informationen, Daten, IT-Systeme und IT-Ressourcen sind gemäß ihrem definierten Schutzniveau so geschützt, dass nur

- erlaubte Zugriffe und erlaubte Veröffentlichungen (Schutzziel: Vertraulichkeit),
- erlaubte Änderungen (Schutzziel: Integrität) und
- erlaubte Löschungen bzw. Unterbrechungen (Schutzziel: Verfügbarkeit)

möglich sind.

Außerdem werden bei geschäftskritischen Verfahren alle sicherheitsrelevanten Vorgänge in erforderlichem Umfange protokolliert und ausgewertet (Schutzziel: Nachvollziehbarkeit).

2. Angemessenheit

Jeder Informationseigentümer - bzw. jeder von diesem Beauftragte - sorgt dafür, dass bei allen Maßnahmen zum Schutz von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen das Wirtschaftlichkeitsprinzip benutzt wird.

Dabei sind die Auswirkungen auf das Betriebsrisiko, d. h. den IT-Betriebskreislauf einerseits und dem IT-Sicherheitskreislauf andererseits (z.B. unerlaubte Zugriffe, unerlaubte Veröffentlichung, unerlaubte Änderung oder Zerstörung von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen) zu bewerten.

Der Aufwand zum Schutz der Informationen steht in einem wirtschaftlich vertretbaren Verhältnis zum Wert der Information für den Hochschulverbund.

3. Zugriffsregelung

Jeder Zugriff auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen des Hochschulverbundes wird genehmigt, kontrolliert und protokolliert.

Der Zugriff begründet sich ausschließlich aus den betrieblichen Erfordernissen der jeweiligen Funktion innerhalb der Hochschule.

Die Beantragung und Vergabe von Benutzerkennungen erfolgt über eine zentrale Berechtigungsverwaltung und wird in einer eigenen Richtlinie beschrieben.

4. Akzeptanz und Verpflichtung

Alle natürlichen und juristischen Personen, die Zugriff auf Informationen, Daten, IT-Systeme und IT-Ressourcen der Hochschule erhalten sollen, akzeptieren formal die Notwendigkeit, die Informationen, Daten, IT-Systeme und IT- Ressource in der Hochschule schützen.

Alle Beschäftigten, Auftragnehmer und andere Dritte sind individuell verpflichtet, diese Anforderung im Rahmen ihrer jeweiligen Funktion aktiv zu unterstützen.

5. Sensibilisierung

Die Hochschulleitung schafft die erforderlichen Rahmenbedingungen, damit alle betroffenen Beschäftigten, Auftragnehmer und andere Dritte die IT-Sicherheitsleitlinie der Hochschule kennen, verstehen und befolgen können.

6. Gesetze und Auflagen

Die Maßnahmen zum Schutz von sensiblen Informationen, Daten, IT-Systemen und IT-Ressourcen entsprechen den jeweils gültigen gesetzlichen Auflagen und Verordnungen.

7. Umgang mit vertraulichen Informationen

Vertrauliche Informationen, Daten und IT-Ressourcen werden so erfasst, verarbeitet und gespeichert, dass ein unerlaubter Zugriff oder Missbrauch ausgeschlossen ist.

Die Erfassung, Verarbeitung und Speicherung von personenbezogenen Daten werden in der Hochschule in einer eigenen Richtlinie geregelt.

8. Integrität der Geschäftsdaten

Die Integrität der zu verarbeitenden geschäftskritischen Daten und Informationen ist durch geeignete technische und organisatorische Maßnahmen während der

- Verarbeitung,
- Speicherung und
- Übertragung

zu gewährleisten.

Dies ist z.B. dann der Fall, wenn nach Abschluss eines Verarbeitungsschrittes die Daten zu einem Dritten übertragen, an ein anderes Verfahren übergeben oder auf ein anderes Medium gespeichert werden (z.B.: Backup/Archivierung).

Die Prüfung der fachlichen Korrektheit und Zulässigkeit der Dateneingabe, Verarbeitung dieser Informationen und der daraus resultierenden Ergebnisse sind in den jeweiligen Verfahrensbeschreibungen festgelegt und nicht Bestandteil dieser IT-Sicherheitsleitlinie.

9. Verantwortung des Informationseigentümers

Jede Information, jede Datei, jedes Verfahren, jedes IT-System und jede IT-Ressource hat einen eindeutig zugeordneten Informationseigentümer.

Dieser ist für die Einstufung des Schutzbedarfs und die Vergabe der Zugriffsberechtigungen verantwortlich.

10. Zugriff entsprechend der Funktion

Für die Vergabe von Zugriffsrechten gibt es einheitliche Regelungen.

Der Zugriff auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen wird entsprechend der jeweiligen Funktion innerhalb der Hochschule vergeben.

11. Unterweisung und Sensibilisierung

Das erforderliche Wissen zur Anwendung der IT-Sicherheitsleitlinie in der Hochschule wird den verschiedenen Zielgruppen (Nutzer, Betreuer, Führungskräfte usw.) in Art und Umfang angemessen zur Verfügung gestellt.

Alle Beschäftigte, Auftragsnehmer und andere Dritte, die Zugriff auf sensible Informationen, Daten, IT-Systeme und IT-Ressourcen der Hochschule haben, werden darüber informiert, wie sie IT-Sicherheitsvorfälle erkennen können und diese entsprechend zu behandeln sind.

Beschäftigte des Hochschulverbundes gelten als vertrauenswürdig, eine Überwachung oder auch nur Verfolgung aller Aktivitäten im Netz ist weder notwendig noch wünschenswert.

12. Integrität des IT-Betriebs- und IT-Sicherheitskreislaufs

Alle relevanten Teile des IT-Betriebskreislaufs und des IT-Sicherheitskreislaufs in der Hochschule werden nach einem geregelten und prüfbaren Verfahren entwickelt oder beschafft, getestet, eingeführt, betrieben, geändert und abgebaut.

13. Erkennen von IT-Sicherheitsverletzungen

Für alle geschäftskritischen Informationen, Daten, Verfahren, IT-Systeme und IT-Ressourcen in der Hochschule sind Mechanismen und Prozesse implementiert, die unberechtigten Zugriffe bzw. unberechtigte Zugriffsversuche zeitnah erkennen.

14. Urheberschaft

Es werden bei den Verfahren und IT-Systemen der Hochschule nur solche Authentifizierungsmethoden eingesetzt, die eine eindeutige Zuordnung zu einer Person oder zu einem Dienst gewährleisten.

15. Protokollierung

Alle IT-sicherheitsrelevanten Vorgänge werden protokolliert. Aufbewahrungs- und Löschfristen richten sich hierbei nach den aktuellen gesetzlichen Vorgaben.

16. Reaktion auf IT-Sicherheitsvorfälle

Alle Vorfälle, die Auswirkungen auf die Schutzziele der IT-Sicherheitsrichtlinie haben, werden dokumentiert, berichtet und in angemessener Art und Weise behandelt.

17. Schwachstellen

Alle geschäftskritischen Verfahren, IT-Systeme und IT-Ressourcen werden regelmäßig auf Sicherheitsschwachstellen untersucht. Dazu wird eine Risikoanalyse erarbeitet.

18. Einhaltung der IT-Sicherheitsleitlinie

Alle Vorgaben der IT-Sicherheitsleitlinie werden regelmäßig überprüft, um sicherzustellen, dass diese - wie vorgesehen - funktionieren und zum Zeitpunkt der Prüfung noch ausreichend sind, um die aktuellen Anforderungen zum Schutz der betroffenen sensiblen Informationen, Daten, IT-Systeme und IT-Ressourcen zu erfüllen.

19. IT-Sicherheitsberichtswesen

Die automatisiert erstellten Protokolle der IT-sicherheitsrelevanten Vorgänge werden regelmäßig und bei Verdacht bzw. bei einem erkannten Sicherheitsvorfall ausgewertet. Die Ergebnisse der Auswertung werden im Rahmen eines definierten und abgestimmten Prozesses intern berichtet.

Alle anderen IT-sicherheitsrelevanten Vorfälle werden manuell erfasst, dokumentiert, kontrolliert und ausgewertet und im Rahmen eines definierten und abgestimmten Prozesses intern berichtet.

20. Notfallplanung

Für die geschäftskritischen IT-Systeme und Verfahren der Hochschule sind die erforderlichen Vorkehrungen zu treffen, um das IT-Betriebsrisiko zu minimieren.

21. Ausnahmen

Aufgrund technischer oder organisatorischer Gegebenheiten kann es bei den IT-Systemen und Verfahren der Hochschule Ausnahmen zu den IT-Sicherheitsvorgaben und IT-Sicherheitsumsetzungsanforderungen geben.

Über diese Ausnahmen wird im Einzelfall in einem geregelten Prozess entschieden, sie werden dokumentiert und nachverfolgt.

22. IT-Sicherheitsumsetzungsanforderungen

Die weitere Detaillierung der IT-Sicherheitsvorgaben findet in den IT-Sicherheitsumsetzungsanforderungen statt.

23. Allgemeines

Verspätete oder fehlerhafte Entscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für die Hochschulleitung bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungs- und Controlling-Daten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.

Die Datenschutzgesetze und die Interessen der Beschäftigten verlangen eine Sicherstellung der Vertraulichkeit der Mitarbeiterdaten. Die Daten und die IT-Anwendungen der Personalabteilung werden daher einem hohen Vertraulichkeitsschutz unterzogen. Gleiches gilt für die Daten der Studierenden.

Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist an der Hochschule selbstverständlich. E-Mail dient als Ersatz oder als Ergänzung von anderen Bürokommunikationswegen. Durch geeignete Maßnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Weiterhin bleiben für den IT-Bereich die Vorgaben aus dem Grundschutzhandbuch (GSHB) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) immer dann verbindlich, sofern keine spezifischen Regelungen für das zu betrachtende IT-Verfahren existieren.

III. IT-Sicherheitsmanagement

Zur Erreichung der IT-Sicherheitsziele wird ein IT-Sicherheitsteam gebildet. Das Team berichtet in seiner Funktion direkt an die jeweilige Hochschulleitung.

Dem IT-Sicherheitsteam und den Administratoren werden von der Hochschule ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren, damit die von der Hochschulleitung festgelegten IT-Sicherheitsziele erreicht werden können.

Die Administratoren und das IT-Sicherheitsteam sind durch die IT-Benutzer ausreichend in ihrer Arbeit zu unterstützen.

Das IT-Sicherheitsteam ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Die IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des IT-Sicherheitsteams zu halten.

Alternativ kann zu dem IT-Sicherheitsteam ein/e IT-Sicherheitsbeauftragte/r ernannt werden. Dieser ist in gleicher Weise zu unterstützen wie das IT-Sicherheitsteam.

Es wurde ein/e Datenschutzbeauftragte/r bestellt. Der oder die Datenschutzbeauftragte hat ein ausreichend bemessenes Zeitbudget für die Erfüllung der Pflichten zur Verfügung. Der oder die Datenschutzbeauftragte ist angehalten, sich regelmäßig weiterzubilden.

IV. Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass eine Vertretung ihre Aufgaben erfüllen kann.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Ziel ist es, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerablen Zeitspanne wiederherzustellen.

Sofern IT-Dienstleistungen an externe Stellen ausgelagert werden, werden konkrete Sicherheitsanforderungen in einem Service-Level-Agreement bzw. in Leistungsbeschreibungen vorgegeben. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben wird ein detailliertes IT-Sicherheitskonzept mit konkreten Vorgaben erstellt.

IT-Benutzer nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Hochschulleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Für den alltäglichen Betrieb der IT-Infrastruktur sind von den Hochschulen Benutzerordnungen zu erlassen, in denen inhärent auch die Sicherheitsrichtlinien geregelt sind.

V. Verbesserung der Sicherheit

Das Managementsystem der IT-Sicherheit wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

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

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem

Ziel analysiert, die IT-Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der IT-Sicherheitstechnik zu halten.

VI. Fortschreibungs- und Berichtspflicht

Die IT-Sicherheitsleitlinie bedarf der ständigen Überarbeitung und Weiterentwicklung. Veränderungen in der Bedrohungssituation oder technische Entwicklungen sind zu berücksichtigen. Turnusmäßig (z.B. im Zusammenhang mit der Fortschreibung der IT-Sicherheitsleitlinie) werden die Aufzeichnungen zu aufgetretenen Sicherheitsproblemen ausgewertet. Bei Bedarf werden zusätzliche Maßnahmen in den Grundschutzkatalog aufgenommen und ggf. auch Maßnahmen wieder aufgehoben bzw. ersetzt, die sich nicht bewährt haben.

Mit der vorliegenden IT-Sicherheitsleitlinie werden Grundlagen und Werkzeuge bereitgestellt, mit deren Hilfe die angestrebte Sicherheit gewährleistet und so schrittweise ein ausreichendes Sicherheitsniveau erreicht werden kann. Dies ist ein kontinuierlicher Prozess, der die konstruktive Zusammenarbeit aller Beteiligten erfordert.

VII. Inkrafttreten, Außenkrafttreten

Die Sicherheitsleitlinie tritt mit der Veröffentlichung im Mitteilungsblatt der Hochschule für Musik „Hanns Eisler“ in Kraft. Sie wird damit für alle Beschäftigten verbindlich. Sie tritt mit Ablauf des 30. November 2014 außer Kraft.

Berlin, den 20. November 2009

Prof. Jörg-Peter Weigle

- Rektor -