13/12

26. April 2012

Amtliches Mitteilungsblatt

Seite

Herausgeber
Die Hochschulleitung der HTW Berlin
Treskowallee 8
10318 Berlin

Redaktion
Rechtsstelle
Tel. +49 30 5019-2813
Fax +49 30 5019-2815

HOCHSCHULE FÜR TECHNIK UND WIRTSCHAFT BERLIN

Grundsätze der Informationssicherheit der HTW Berlin

(beschlossen von der Hochschulleitung am 18.04.2012)

Inhalt

1. Einleitung

Die Grundsätze der Informationssicherheit der HTW Berlin beschreiben die Bedeutung der Informationsverarbeitung, die Sicherheitsziele, das Informationssicherheitsmanagement sowie Aspekte der Durchsetzung und Aufrechterhaltung des Sicherheitsniveaus und den Umgang mit Ausnahmen. Hiermit werden anzuwendende Standards und Rahmenbedingungen für einen sicheren Betrieb der Informationstechnik (IT) und den sicheren Umgang mit Informationen festgelegt.

Bedingung für den Erfolg ist ein Ausgleich zwischen akademischer Freiheit und Informationssicherheit.

2. Bedeutung der Informationssicherheit

Die Informationsverarbeitung ist ein wesentlicher Kernprozess zur Erreichung der Ziele der HTW Berlin. Die wesentlichen Organisationsabläufe sind in starkem Maße von einer sicheren und funktionierenden Informationsverarbeitung abhängig. Die technische Durchdringung und Verflechtung von bzw. zwischen internen Prozessen und externen Beziehungen der HTW Berlin schreitet fort.

Die Hochschulleitung der HTW Berlin ist sich der damit einhergehenden Verantwortung bewusst. Durch Initiierung, Umsetzung und Aufrechterhaltung des Informationssicherheitsprozesses wird sie entsprechenden Anforderungen gerecht und übernimmt die Gesamtverantwortung für einen angemessenen Umgang mit Informationen.

3. Zweck, Geltungsbereich und Verantwortlichkeiten

Die Hochschulleitung der HTW Berlin verabschiedet hiermit diese Grundsätze der Informationssicherheit im Sinne einer Leitlinie. Übergeordnetes Ziel ist es, ein angemessenes Maß an Informationssicherheit zu erreichen und aufrecht zu erhalten.

Für die Einhaltung und Umsetzung dieser Leitlinie ist jedes Mitglied der HTW Berlin verantwortlich. Die Hochschulleitung und die Führungskräfte der HTW Berlin unterstützen den Informationssicherheitsprozess und überwachen die Einhaltung dieser Regelungen aktiv.

4. Sicherheitsziele

Aus den Anforderungen, die die Aufgaben der HTW Berlin mit sich bringen sowie den einzuhaltenden gesetzlichen, regulatorischen und vertraglichen Verpflichtungen leiten sich die Sicherheitsziele hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der eingesetzten informationsverarbeitenden Systeme und Prozesse ab.
Alle Sicherheitsmaßnahmen müssen in einem finanziell vertretbaren Verhältnis zum Wert der schützenswerten Informationen, der informationsverarbeitenden Systeme und Prozesse stehen.

Ereignisse mit negativen finanziellen, aber auch immateriellen Auswirkungen durch fehlende Informationssicherheit müssen verhindert werden.

5. Informationssicherheitsmanagement

Zur Erreichung der Sicherheitsziele wird ein Informationssicherheitsmanagementsystem eingerichtet, das primär gemäß der Vorgaben der Standards 100-1 „Managementsysteme für Informationssicherheit (ISMS)“ und 100-2 „IT-Grundschutz-Vorgehensweise“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) geplant, implementiert, betrieben und aufrecht erhalten wird.

Zu diesem Zweck wurde eine Informationssicherheitsorganisation eingerichtet. Es ist ein/e Informationssicherheitsbeauftragte/r benannt worden. Der/Die Informationssicherheitsbeauftragte berichtet in seiner/ihrer Funktion direkt an die Hochschulleitung.
Der/Die Informationssicherheitsbeauftragte ist zuständig für die Ableitung der notwendigen infrastrukturellen, technischen, organisatorischen und personellen Sicherheitsmaßnahmen, gemessen an den Zielen und Anforderungen an die Informationen und informationsverarbeitenden Systeme und Prozesse. Er/Sie legt diese gemeinsam mit der ZE HRZ (Zentraleinrichtung Hochschulrechenzentrum) konzeptionell in spezifischen Sicherheitskonzepten nieder, kontrolliert regelmäßig deren Umsetzung bzw. Einhaltung und schreibt sie bedarfsgerecht fort.

Dem/der Informationssicherheitsbeauftragten und der ZE HRZ werden von der Hochschulleitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren, um die festgelegten Sicherheitsziele zu erreichen.

Der/die Informationssicherheitsbeauftragte und die ZE HRZ sind durch die IT-Benutzer/innen ausreichend in ihrer Tätigkeit zu unterstützen. Die IT-Benutzer/innen haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des/der Informationssicherheitsbeauftragten zu halten.

Der/die Informationssicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um bereits in der Planungsphase Sicherheitsaspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den/die Datenschutzbeauftragte/n.
Der/die Datenschutzbeauftragte der HTW Berlin hat ein ausreichendes Zeitbudget für die Erfüllung seiner/ihrer Pflichten zur Verfügung und ist ebenfalls gehalten, sich regelmäßig weiterzubilden.

Für alle Verfahren, Informationen, IT-Anwendungen, IT-Systeme und Räumlichkeiten sind bzw. werden verantwortliche Personen benannt. Diese arbeiten eng mit dem/der Informationssicherheitsbeauftragten zusammen.

Für alle zur Erreichung der Ziele der Hochschule relevanten Informationen, IT-Anwendungen, IT-Systeme und Räumlichkeiten erfolgt eine Ermittlung des Schutzbedarfs sowie eine Auswahl und Umsetzung von angemessenen Sicherheitsmaßnahmen. Dabei werden die Standards und Grundschutz-Kataloge des BSI angewendet. Die Vorgehensweise, Maßnahmen und Ergebnisse werden im Informationssicherheitskonzept dokumentiert.

6. Durchsetzung und Aufrechterhaltung

Die für die Umsetzung und Kontrolle der Informationssicherheitsmaßnahmen erforderlichen, personellen und technischen Ressourcen und Investitionsmittel werden von der Hochschulleitung bereitgestellt.

Diese Grundsätze der Informationssicherheit werden durch zusätzliche Sicherheitskonzepte, Richtlinien und Regelungen sowie Anweisungen für die Benutzer konkretisiert.

Die Grundsätze der Informationssicherheit und damit in Zusammenhang stehende Regelungen werden jährlich hinsichtlich ihrer Wirksamkeit und Angemessenheit überprüft und bei Bedarf angepasst. Die Überprüfung und Anpassung wird durch den/die Informationssicherheitsbeauftragte/n im Rahmen des Sicherheitsprozesses initiiert. Die Hochschulleitung wird über die Ergebnisse unterrichtet und aktiv in den Änderungs- bzw. Anpassungsprozess eingebunden. Die Ergebnisse werden dokumentiert und den betreffenden Mitgliedern der HTW Berlin zur Kenntnis gegeben.

7. Ausnahmen

Ausnahmen von diesen Grundsätzen der Informationssicherheit und den mit diesen im Zusammenhang stehenden Regelungen sind zulässig, sofern diese keine negativen Auswirkungen auf die Erreichung der Informationssicherheitsziele und der Ziele der HTW Berlin haben. Hierzu ist eine Bewertung der Auswirkungen vorzunehmen und eine Genehmigung des/der jeweiligen Vorgesetzten schriftlich einzuholen. Die Ausnahmen sind zu dokumentieren und den betreffenden Mitgliedern der HTW Berlin zur Kenntnis zu geben.

8. Weitere Regelungen zur Informationssicherheit

Die vorstehenden Grundsätze und deren Ziele werden im Informationssicherheitskonzept und allen damit im Zusammenhang stehenden Regelungen und Anweisungen umgesetzt und sind für die Mitglieder der HTW Berlin bindend.

9. Inkrafttreten

Diese Grundsätze treten am Tag nach ihrer Veröffentlichung im Amtlichen Mitteilungsblatt der HTW Berlin in Kraft.