Technische Hochschule Brandenburg
University of Applied Sciences

07.12.2017 **Amtliche Mitteilungen der Technischen Hochschule Brandenburg** **25. Jahrgang**
Nummer 33

Datum	**Inhalt**	**Seite**

Herausgeber
Die Präsidentin
Technische Hochschule Brandenburg
Körperschaft des öffentlichen Rechts

Technische Hochschule Brandenburg
Magdeburger Str. 50
14770 Brandenburg an der Havel
T +49 3381 355 – 0, F +49 3381 355 - 199

IT-Sicherheitsleitlinie der Technischen Hochschule Brandenburg[1]

Inhaltsverzeichnis

[1] Diese Sicherheitsleitlinie basiert wesentlich auf dem Dokument „IT-Sicherheitspolitik" der Fachhochschule Flensburg, das von der AG IT-Sicherheit der teilnehmenden Forschungseinrichtungen und Hochschulen des Landes Schleswig-Holstein am 08.10.2010 veröffentlicht wurde. Die IT Sicherheitsleitlinie wurde in den Sitzungen der IT-Kommission der Technischen Hochschule Brandenburg beraten, vom Präsidium am 15.03.2017 verabschiedet und am 05.04.2017 vom Senat zur Kenntnis genommen.

Präambel

Für die Aufgabenerfüllung von Hochschulen und Forschungseinrichtungen sind Dienstleistungen der Informations- und Kommunikationstechnik (IKT bzw. IT) von zunehmender Bedeutung. Damit nimmt auch die Abhängigkeit dieser von der Funktionstüchtigkeit einer IKT stetig zu. Es ist daher unerlässlich, umfassende Schutzmaßnahmen zu ergreifen. Dieses Papier definiert die IT-Sicherheitspolitik der Hochschulen und Forschungseinrichtungen. Es stellt die Basis für eine IT-Sicherheitsrichtlinie und darauf folgender Maßnahmen für eine schrittweise Verbesserung und dauerhafte Aufrechterhaltung der Sicherheit im Bereich der Informationstechnik dar. Dabei sollte berücksichtigt werden:

Der Auftwand für die IT-Sicherheitsmaßnahmen ist in Relation zu dem erzielten Sicherheitsgewinn und dem Wert der zu schützenden Güter zu setzen.

IT-Sicherheitsziele und Maßnahmen orientieren sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). IT-Sicherheit umfasst die Verfügbarkeit, Integrität und Vertraulichkeit von Daten und Anwendungen. Technische Systeme verfügen über eine begrenzte Verfügbarkeit und bieten Möglichkeiten der Manipulation und des Vertraulichkeitsverlustes. Gegen diese Bedrohungen sind geeignete Maßnahmen zu ergreifen.

Aufgrund der Bedeutung der IKT wird die Realisierung und Einhaltung der IT-Sicherheit durch das Präsidium der Hochschule unterstützt. Darüber hinaus wirkt das Präsidium darauf hin, dass im Rahmen der Kooperation der Hochschulen des Landes Brandenburg die Ausarbeitung von IT-Sicherheitsrichtlinien sowie zugehöriger Maßnahmenkataloge abgestimmt wird.

Die folgenden Ausführungen definieren die IT-Sicherheitsleitlinie für die Hochschule, welche die Basis für ein zu erarbeitendes IT-Sicherheitskonzept sowie daraus abzuleitender Maßnahmen darstellt. Bei dauernd wechselnden Gefährdungen ist die Aufrechterhaltung der IT-Sicherheit eine permanente Aufgabe. Dieses erfordert personelle und finanzielle Mittel und die Mitwirkung jedes Einzelnen.

Die Geltungsdauer dieses Dokuments beträgt zunächst 10 Jahre, ggf. wird es durch ein landesweit zu verabschiedendes Dokument ersetzt.

1 Bedeutung der Informations- und Kommunikationstechnik

Die Informations- und Kommunikationstechnik ist von zentraler Bedeutung für die Aufgabenerfüllung der Hochschulen und Forschungseinrichtungen. Das Spektrum der IT-Anwendungen umfasst die rechnergestützte Informationsverarbeitung für Forschung, Lehre, Studium und Verwaltung sowie die Kommunikation mit externen Partnern und Auftraggebern. Die Bedeutung der Informationstechnik für die unterschiedlichen Anwendungsgebiete ist unterschiedlich hoch. Dementsprechend sind die Auswirkungen von Störungen oder Ausfällen in den verschiedenen Anwendungsgebieten von unterschiedlicher Tragweite.

2 IT-Sicherheitsziele

Lösungen zur Erreichung von IT-Sicherheitszielen sollen das Restrisiko verkleinern, müssen angemessen und wirtschaftlich vertretbar sein. IT-Sicherheitsziele sind die Verfügbarkeit von IKT, die Integrität und Vertraulichkeit von Daten sowie die Einhaltung gesetzlicher Auflagen.

2.1 Verfügbarkeit

Technische Systeme besitzen eine begrenzte Verfügbarkeit. Dabei ist organisatorisch festzulegen, welche Ausfallzeiten akzeptabel und unter dem Gesichtspunkt der Wirtschaftlichkeit vertretbar sind. In Abhängigkeit dieser Forderungen sind geeignete Maßnahmen zu ergreifen, die in den akzeptierten zeitlichen Grenzen einen Wiederanlauf ermöglichen. Daten sind in mehrstufigen Verfahren so zu sichern, damit nach menschlichem Ermessen ein grundsätzlicher Verlust ausgeschlossen werden kann.

2.2 Integrität von Daten

Unbefugte oder unbemerkte Veränderungen von Daten sollen ausgeschlossen sein, sei es durch Personen oder technische Fehler. Es wird erwartet, dass Daten weder irrtümlich noch mutwillig manipuliert werden. Je nach Anwendung sind deshalb geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Integrität von Daten zu erhalten.

2.3 Vertraulichkeit von Daten

Die Hochschule verarbeitet unterschiedlichste vertrauliche Informationen. Da nicht ausgeschlossen ist, dass auf die Daten unberechtigt zugegriffen wird, müssen geeignete technische, organisatorische und personelle Maßnahmen in den Anwendungen, dem IT-Netz, den Arbeitsplatzcomputern und auf den Übertragungswegen ergriffen werden, die einen möglichst effektiven Zugriffsschutz bewirken.

2.4 Einhaltung gesetzlicher Auflagen

Die Hochschule hat eine Vielzahl gesetzlicher Auflagen, wie Datenschutz, Arbeits- und IT-Sicherheit etc. zu erfüllen. IT-Systeme und die dazu erlassenen organisatorischen Regelungen müssen so ausgelegt sein, dass die gesetzlichen Bestimmungen eingehalten werden und die Compliance jederzeit nachgewiesen werden kann.

3 Aufgabenzuordnung

Die Gesamtverantwortung für die IT-Sicherheit an der Hochschule liegt beim Präsidium. Bei allen hochschulweiten Entscheidungen zur IT-Sicherheit wird das Präsidium von der Ständigen IT-Kommission beraten und unterstützt.

3.1 IT-Sicherheitsbeauftragte(r)

Das Präsidium bestellt zum nächstmöglichen Zeitpunkt eine IT-Sicherheitsbeauftragte oder einen IT-Sicherheitsbeauftragten.

Die oder der IT-Sicherheitsbeauftragte ist dafür zuständig, dass die in dieser IT-Sicherheitsleitlinie genannten Ziele umgesetzt werden. Sie oder er sorgt dafür, dass angemessene IT-Sicherheitsmaßnahmen realisiert, fortentwickelt und überwacht werden.

Sich hieraus ergebende Regeln sind für alle Nutzerinnen und Nutzer der IT-Infrastruktur verbindlich.

3.2 Datenschutzbeauftragte(r)

Das Präsidium bestellt eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. Eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter muss bestellt werden, wenn personenbezogene Daten (z. B. Arbeitnehmerdaten in der Personalabteilung, Kunden- und Interessentendaten) automatisiert verarbeitet werden.

3.3 Geltungsbereich

Jede Nutzerin und jeder Nutzer der Informations- und Kommunikationstechnik ist für die Sicherheit und den Schutz der Daten in ihrem oder seinem Verantwortungsbereich verantwortlich. Alle Mitglieder und Angehörigen der Hochschule sind verpflichtet, bei der Erfüllung der Aufgabe „IT-Sicherheit" kooperativ und verantwortungsbewusst mitzuwirken.

4 IT-Sicherheitsrichtlinien und Maßnahmenkatalog

Die oder der IT-Sicherheitsbeauftragte verantwortet die Erstellung und Pflege der IT-Sicherheitsrichtlinien und die Umsetzung der dort aufgeführten Maßnahmenkataloge. Dabei orientiert sie oder er sich ggf. an landesweiten Empfehlungen der IT-Arbeitsgruppe der Hochschule des Landes Brandenburg.

5 In-Kraft-Treten

Die IT-Sicherheitsleitlinie tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Mitteilungen in Kraft.

Brandenburg an der Havel, 07.12.2017

gez. Prof. Dr.-Ing. Burghilde Wieneke-Toutaoui
Präsidentin