Technische Hochschule Brandenburg
University of Applied Sciences

16.06.2021 **Amtliche Mitteilungen der Technischen Hochschule Brandenburg** **29. Jahrgang**
Nummer 13

Datum	**Inhalt**	**Seite**

Herausgeber
Der Präsident
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

Leitlinie zur Informationssicherheit der Technischen Hochschule Brandenburg

Inhaltsverzeichnis

Einleitung

Die Technische Hochschule Brandenburg (Hochschule) etabliert ein Managementsystem für Informationssicherheit (ISMS), das dem Regelwerk „IT-Grundschutz" des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügt. Zentraler Bestandteil eines ISMS ist die Leitlinie zur Informationssicherheit. Das vorliegende Dokument ist die Leitlinie zur Informationssicherheit der Hochschule.

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. Grundsätzlich steigen die Abhängigkeiten von Informationstechnik weiter, da die Digitalisierung der Hochschulprozesse proaktiv vorangetrieben wird.

Die Hochschulleitung erkennt, dass sich die Risiken und die zu erwartenden Auswirkungen bei der Informationsverarbeitung verändern und für die Hochschule eine Existenzbedrohung annehmen können. Mit der Leitlinie unterstreicht die Hochschulleitung die Bedeutung der Informationssicherheit für die Hochschule und bestätigt die Übernahme der Gesamtverantwortung für den Informationssicherheitsprozess.

2 Einbettung des ISMS der Hochschule

Als übergeordnetes ISMS fungiert das Ressort-ISMS mit seiner „IT-Sicherheitsrichtlinie für den Geschäftsbereich des MWFK"[1]. Mittelbar bettet sich hierüber das ISMS der Hochschule in das ISMS für die Landesverwaltung Brandenburg mit seiner „Leitlinie für die Informationssicherheit in der Landesverwaltung Brandenburg"[2] ein. Sowohl Ressort-Richtlinie als auch Leitlinie für die Landesverwaltung sind für Hochschulen des Landes Brandenburg nicht verbindlich, sondern fungieren nur als Empfehlungen.

3 Sicherheitsziele

Anforderungen und Maßnahmen zur Erreichung der IT-Sicherheitsziele sollen angemessen und wirtschaftlich vertretbar sein. Die Sicherheitsziele der Hochschule sind:

- Zuverlässige Unterstützung der Geschäftsprozesse durch die IT und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation,
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Einhaltung der aus gesetzlichen Vorgaben resultierenden Anforderungen,

[1] Version von Juli 2017
[2] Version 1.0 vom 14.04.2014

- Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der Verarbeitung personenbezogener Daten,
- Reduzierung der im Schadensfall entstehenden Kosten sowie Wahrung besonderer Dienst- oder Amtsgeheimnisse.

Für die Erreichung der Sicherheitsziele sollen die Grundwerte Verfügbarkeit von Informations- und Kommunikations-Technik (IKT) sowie die Integrität und Vertraulichkeit von Daten herangezogen werden.

4 Geltungsbereich

Diese Leitlinie und somit das Informationssicherheitsmanagement-System (ISMS) der Hochschule ist verbindlich für sämtliche Hochschulmitglieder und alle organisatorischen Einheiten der Hochschule; es umfasst sämtliche Geschäftsprozesse aus Lehre, Forschung und Verwaltung. Es zielt technisch sowohl auf die zentral vom Hochschulrechenzentrum betriebene IT als auch auf die dezentrale IT (betrieben durch die Fachbereiche) ab. Örtlich sind neben dem Hauptstandort auch Agentur Duales Studium, die Präsenzstellen und etwaig weitere Organisationseinheiten integriert, soweit sie von der Hochschule verantwortet werden.

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.

Die Leitlinie ist auch von von der Hochschule beauftragten Dienstleistern verpflichtend einzuhalten. Bei IT-Dienstleistungen, die von externen Stellen erbracht werden, müssen die Leistungsvereinbarungen Vorgaben zu konkreten Sicherheitsanforderungen enthalten.

5 Organisation der Informationssicherheit

Die Gesamtverantwortung für die Informationssicherheit an der Hochschule liegt bei der Präsidentin oder dem Präsidenten. Bei allen hochschulweiten Entscheidungen zur Informationssicherheit wird die Präsidentin oder der Präsident von der oder von dem Informationssicherheitsbeauftragten beraten und unterstützt.

5.1 Informationssicherheitsbeauftragte(r)

Die Präsidentin oder der Präsident bestellt eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (ISB).

Die oder der ISB steuert den Sicherheitsprozess, damit die in dieser Leitlinie genannten Ziele umgesetzt werden können. Sie oder er wirkt darauf hin, dass angemessene IT-Sicherheitsmaßnahmen realisiert, fortentwickelt und überwacht werden.

6 Umsetzung und Sicherheitsrichtlinien

Nutzerinnen und Nutzer sind bei der Erstellung, Nutzung und Verwaltung von Informationen verpflichtet, die Informationssicherheitsleitlinie und mitgeltende Dokumente (Richtlinien) einzuhalten.

Die Präsidentin oder der Präsident beauftragt die oder den ISB, geeignete Maßnahmen im Sinne der Informationssicherheitsleitlinie zu treffen, um die Sicherheitsziele zu erreichen.

Maßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Information und IT-Systeme liegen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.

6.1 Vorgehensweise und Sicherheitskonzeption

Für die Umsetzung des Informationssicherheitsmanagements kommt die Vorgehensweise des IT-Grundschutz (BSI 200-2 /200-3) zur Anwendung. Dabei ist das IT-Grundschutzkompendium des BSI in der jeweils aktuellen Version als Maßnahmenkatalog zugrunde zu legen. Langfristig wird eine Standardabsicherung des gesamten Geltungsbereichs angestrebt; im ersten Schritt wird die Kernabsicherung der Prozessbausteine und der zentralen IT angestrebt. Die oder der ISB steuert die Erstellung der Sicherheitskonzeption.

Risiken im Sinne der Informationssicherheit sollen derart aufbereitet werden, dass die Präsidentin oder der Präsident auf der Basis bewusst steuern kann. Optionen zur Behandlung der Risiken sind die Ergreifung geeigneter Maßnahmen zur Verminderung der Risiken, die bewusste und objektive Akzeptanz der Risiken und die Übertragung der Risiken auf Dienstleister beziehungsweise Versicherungen. Weitere Details sind in einer Richtlinie zu regeln.

6.2 Richtlinien

Die oder der Informationssicherheitsbeauftragte verantwortet die Erstellung und Pflege der Sicherheitsrichtlinien und der Sicherheitsanforderungen. Er oder sie stützt sich dabei auf Zuarbeiten aus anderen Bereichen ab.
Insbesondere sind laut Vorgabe für das Land Brandenburg ein Virenschutzkonzept, ein Datensicherungs- und Archivierungskonzept, ein Notfallvorsorgekonzept und Sicherheitsregeln für die IT-Nutzung zu erarbeiten.

6.3 Verfahrensverantwortung und Informationseigner

Zu jedem IT-gestützten Geschäftsprozess und jedem Fachverfahren muss in Verantwortung der Organisationseinheit eine Ansprechpartnerin oder ein Ansprechpartner benannt werden, die oder der als sogenannter Informationseigentümer (Verfahrensverantwortliche) für alle Fragen der Informationsverarbeitung und der Informationssicherheit im Rahmen dieses Fachverfahrens verantwortlich ist. Diese Verantwortung beinhaltet die Festlegung der Zugriffsrechte auf die Informationen, die für die Nutzerinnen und Nutzer im Rahmen des Geschäftsbedarfs erforderlich sind. Die oder der Verantwortliche für einen Geschäftsprozess muss sicherstellen, dass die Sicherheitsanforderungen dem Schutzbedarf entsprechen. Die hierfür erforderlichen Schutzbedarfs-Definitionen sind vom oder von der ISB bereitzustellen.

6.4 Einbindung aller Mitarbeiter in den Sicherheitsprozess

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiterinnen und Mitarbeiter. Jede und jeder Einzelne kann durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden zu

vermeiden und zum Erfolg beitragen. Die oder der ISB wird Sensibilisierungen für Informationssicherheit und fachliche Schulungen der Mitarbeiterinnen und Mitarbeiter durchführen, da sie eine Grundvoraussetzung für Informationssicherheit sind.

Mitarbeiterinnen und Mitarbeiter müssen über den Sinn von Sicherheitsmaßnahmen aufgeklärt werden. Dies ist besonders wichtig, wenn sie Komfort- oder Funktionseinbußen zur Folge haben. Die Sicherheitsmaßnahmen sollten für die Anwenderin und den Anwender transparent und verständlich sein, sofern dadurch kein Sicherheitsrisiko entsteht.

6.5 Meldung von Sicherheitsvorfällen

Die oder der ISB richtet eine Meldestelle zur Meldung von sicherheitsrelevanten Ereignissen ein. Alle Mitarbeiterinnen und Mitarbeiter melden entsprechende Ereignisse über diese Meldestelle. Die oder der ISB konkretisiert die Rahmenbedingungen für die Meldestelle (insbesondere Definitionen und Schwellenwerte) in einer Richtlinie.

Bei erkennbar erheblicher Gefahr der Verletzung der Informationssicherheit kann die oder der ISB die sofortige beziehungsweise vorübergehende Stelllegung des betroffenen IT-Systems anordnen sowie die verantwortlichen Benutzerinnen oder Benutzer vorübergehend von der Nutzung der Informationstechnik ausschließen.

7 Überwachung des ISMS und kontinuierliche Verbesserung

Zur Sicherstellung der Qualität des ISMS kommt für den Sicherheitsprozess das PDCA-Modell mit den Phasen Planen, Durchführen, Überwachen und Optimieren zur Anwendung.

7.1 Audits und Revisionen

Die oder der ISB darf sich Überblick über die Informationssicherheit in allen Bereichen der Hochschule verschaffen.
Die oder der ISB überprüft regelmäßig die Wirksamkeit des ISMS. Sie oder er kann dazu Penetrationstests oder angemessene Sicherheitsrevisionen bzw. Sicherheits-Audits durchführen. Die Sicherheitsrevisionen bzw. Sicherheits-Audits müssen dabei auf Grundlage des entsprechenden BSI-Leitfadens durchgeführt werden. Die oder der ISB wertet mit der betroffenen Ansprechpartnerin oder dem betroffenen Ansprechpartner die vorgenommenen Sicherheitsrevisionen/Sicherheits-Audits aus und entwickelt mit ihr oder ihm gemeinsam einen Behandlungsplan der dabei festgestellten Risiken.

7.2 Management-Bericht

Unter Berücksichtigung der Sicherheitsrevisionen/Sicherheits-Auditergebnisse, der Sicherheitsvorfälle, und weiterführender Erkenntnisse aus dem ISM erstellt die oder der ISB einen jährlichen Informationssicherheitsbericht und die Jahresplanung für das Folgejahr und legt diesen der Präsidentin oder dem Präsidenten zum Beschluss vor.

7.3 Kontinuierliche Verbesserung

Die oder der ISB überprüft in regelmäßigen Abständen, ob:

- sich Rahmenbedingungen geändert haben, die dazu führen, dass das Vorgehen in Bezug auf Informationssicherheit geändert werden muss,
- die Sicherheitsziele noch angemessen sind und ob
- die Informationssicherheitsleitlinie noch aktuell ist.

8 In-Kraft-Treten

Die Leitlinie zur Informationssicherheit tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Mitteilungen in Kraft. Gleichzeitig tritt die IT-Sicherheitsleitlinie (Amtliche Mitteilungen der Technischen Hochschule Brandenburg Nr. 33/2017 vom 07.12.20217, Seite 3874) außer Kraft.

Brandenburg an der Havel, 16.06.2021

gez. Prof. Dr. Andreas Wilms
Präsident