Technische Hochschule Wildau
Technical University of Applied Sciences

Amtliche Mitteilungen Nr. 38/2020 18.12.2020

Leitlinie
zum Thema
Informationssicherheit
an der
Technischen Hochschule Wildau

Veröffentlicht: 18.12.2020

Version 1.3

Herausgeberin:
Die Präsidentin
Technische Hochschule Wildau
Körperschaft des öffentlichen Rechts

Hochschulring 1
15745 Wildau
Tel.: 03375/508-0
praesidentin@th-wildau.de

Inhaltsverzeichnis

Stellenwert der Informationsverarbeitung

Der mit Hilfe geeigneter Informations- und Kommunikationstechnik durchgeführten Verarbeitung von Informationen kommt an Hochschulen eine Schlüsselrolle bei der Erfüllung der Aufgaben in Studium und Lehre, Forschung und Transfer sowie in der Administration zu.

Alle Bereiche der Technischen Hochschule Wildau verarbeiten in ihren Prozessen, Verfahren oder Abläufen Informationen. Die Hochschulleitung erkennt, dass sich die Risiken und die zu erwartenden Auswirkungen bei der Informationsverarbeitung verändern und im schlimmsten Fall für die Hochschule eine existenzielle Bedrohung darstellen können.

Mit der Amtlichen Mitteilung 44/2017 unterstreicht die Hochschulleitung die Bedeutung der Informationssicherheit für die Hochschule und bestätigt die Übernahme der Gesamtverantwortung für den Informationssicherheitsprozess.

Die vorliegende Leitlinie beschreibt die allgemeinen Grundsätze, Ziele und Sicherheitsmaßnahmen, die für die Initiierung, Etablierung und Aufrechterhaltung eines ganzheitlichen Informationssicherheitsprozesses an der TH Wildau erforderlich sind.

Grundsätze der Informationssicherheit

Ziel der Informationssicherheit ist es, die Risiken, die auf die folgenden drei Grundwerte einwirken, auf ein vertretbares Maß zu reduzieren. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.

Die Grundwerte der Informationssicherheit lauten:

Vertraulichkeit:
Vertrauliche Informationen sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Nachrichteninhalte und die Informationen über den Kommunikationsvorgang (Wer? Was? Wann? etc.).

Integrität:
Der Begriff der Integrität bezieht sich sowohl auf Informationen als auch auf IT-Systeme. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. In Bezug auf IT-Systeme bezeichnet die Integrität die vollständige und unveränderte Funktionsweise der Systeme.

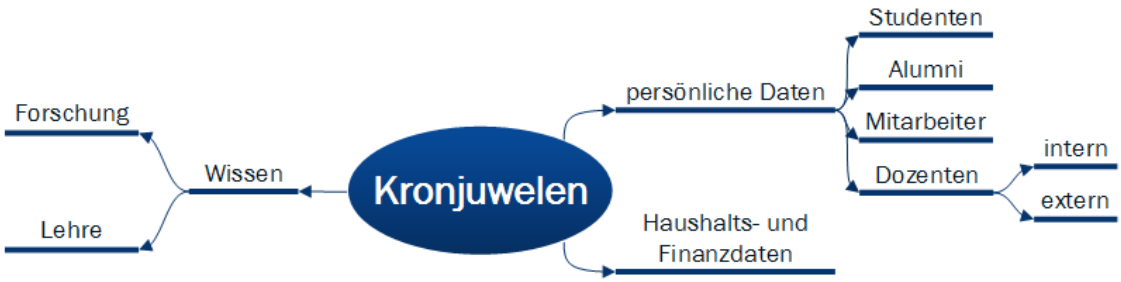
Verfügbarkeit:
Die notwendigen Informationen stehen den Anwendenden zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

Übergreifende Ziele

Um an der TH Wildau die Informationssicherheit zu gewährleisten, müssen diejenigen Informationen der Hochschule identifiziert werden, die sie existenziell bedrohen könnten. Diese werden in einer Bedrohungsanalyse identifiziert und stellen die sogenannten „Kronjuwelen" der TH Wildau dar. Ziel ist es, diejenigen Informationen der Hochschule zu identifizieren, die durch Bekanntwerden, Diebstahl, Zerstörung oder Kompromittierung geeignet sind, einen erheblichen Schaden zu verursachen. Als Schaden für die Hochschule sind sowohl Auswirkungen auf Ansehen und Reputation als auch finanzielle Folgen zu sehen.

Für die TH Wildau sind die identifizierten „Kronjuwelen“:

- Wissen
- persönliche Daten
- Haushalts- und Finanzdaten



Die Bedeutung der „Kronjuwelen“ für die Hochschule wird nachfolgend erläutert.

Wissen:

Nach dem Brandenburgischen Hochschulgesetz § 3 (1) dienen die Hochschulen „...der Pflege und Entwicklung der Wissenschaften und Künste durch Lehre, Forschung, Studium und Weiterbildung“ und sind somit für die Durchführung von Lehre und Forschung verantwortlich. Lehre und Forschung sind folglich die elementaren Kernbereiche der Hochschule. Das dort hervorgebrachte Wissen stellt somit einen Teil ihrer „Kronjuwelen“ dar.

Persönliche Daten:

Der Aspekt der persönlichen Daten setzt sich aus zwei Teilen zusammen.

Zunächst handelt es sich um Zugangsdaten, im Speziellen die Zugangskennung und das dazugehörige Passwort. Der Verlust dieser Daten stellt ein erhebliches Schadenspotenzial für die Hochschule dar.

Weiterhin gilt es, die personenbezogenen Daten zu schützen. Existenzbedrohend ist an diesen Informationen nicht primär der monetäre Schaden, der bei einer Datenschutzverletzung zu erwarten ist. Viel schwerer und nicht abschätzbar sind die negativen Auswirkungen auf das Image, wenn Unzulänglichkeiten im Bereich der personenbezogenen Daten bekannt werden.

Haushalts- und Finanzdaten:

Der unberechtigte Zugang zu Haushalts- oder Finanzdaten der Hochschule stellt ein existenzbedrohendes Risiko dar. Insbesondere dann, wenn diese möglicherweise manipuliert werden können.

Das Primärziel der Informationssicherheit ist die Wahrung von *Vertraulichkeit*, *Verfügbarkeit* und *Integrität* dieser „Kronjuwelen".

Die *Verfügbarkeit* von Prozessen, Verfahren oder Abläufen, die die definierten „Kronjuwelen" verarbeiten, ist so zu sichern, dass kurzfristig Einschränkungen oder Beeinträchtigungen kompensiert werden können.

Fehlfunktionen und Unregelmäßigkeiten sind in Bezug auf die *Integrität* der Informationen und IT-Systeme nur in geringem Umfang und nur in Ausnahmefällen akzeptabel. Die Anforderungen der Informationen an die *Vertraulichkeit* haben ein normales, an der Gesetzeskonformität orientiertes Niveau.

Detailziele

Die Hochschulleitung betreibt ein Informationssicherheitsmanagementsystem (ISMS). Dieses soll die Standards nach ISO27001 erfüllen und wird daher regelmäßig von Externen auditiert. Verantwortlichkeiten für Aufgaben in der Informationssicherheit werden im Informationssicherheitsmanagementsystem vom Informationssicherheitsteam (IST)[1] gepflegt.

In den Sicherheitsprozess sollen schrittweise alle Organisationseinheiten der TH Wildau einbezogen werden, damit das Primärziel sicher zu realisieren ist.

Im Rahmen der bereits angeführten Bedrohungsanalyse sind die Organisationseinheiten der TH Wildau anhand ihrer Aufgaben fortlaufend daraufhin zu überprüfen, inwieweit sie die als „Kronjuwelen" definierten Informationen verarbeiten. Auf Basis dieser Bedrohungsanalyse wird durch die Hochschulleitung eine Priorisierung der Organisationseinheiten bei der Einbeziehung in den Informationssicherheitsprozess vorgenommen. Im Sinne einer iterativen Vorgehensweise wird der Sicherheitsprozess in den Organisationseinheiten schrittweise etabliert.

Der Informationssicherheitsprozess wird in das Prozessmanagement der Hochschule integriert. Ziel hierbei ist es, die für die Informationssicherheit relevanten Informationen in der Prozessdokumentation zu berücksichtigen.

Informationssicherheit kann an der Hochschule nur etabliert werden, wenn alle Angehörigen der Hochschule aktiv mitwirken. Erklärtes Ziel ist es, alle Angehörigen der Hochschule im erforderlichen Umfang zu sensibilisieren und zu qualifizieren, um notwendige Kompetenzen bezüglich der Informationssicherheit aufzubauen bzw. zu vertiefen.

Die umzusetzenden Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch einen Sicherheitsvorfall erwartet wird. Zu bewerten sind dabei die Auswirkungen des Sicherheitsvorfalls auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens der Hochschule sowie die Folgen von Gesetzesverstößen und Beeinträchtigungen der Aufgabenerfüllung.

Informationssicherheitsmanagement

Zur Erreichung der Informationssicherheitsziele wurde eine Sicherheitsorganisation eingerichtet.

Hochschulleitung

Sie ist aufgrund ihrer Gesamtverantwortung für die Risikovorsorge an der Hochschule auch für die Informationssicherheit verantwortlich. Die Hochschulleitung erlässt verbindliche Regeln zur Informationssicherheit für die TH Wildau und gibt sie den Mitarbeitenden und Studierenden bekannt. Diese Regeln werden auf der Webseite unter dem Punkt Informationssicherheit[2] in Form von Informationsmaterialien und Anleitungen abgelegt.

[1] https://www.th-wildau.de/informationssicherheit

[2] https://www.th-wildau.de/informationssicherheit

Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher. Zudem werden von der Hochschulleitung benötigte Ressourcen für die Informationssicherheit bereitgestellt.

Informationssicherheitsteam (IST)

Die Hochschulleitung richtet ein Informationssicherheitsteam (IST) ein. Aufgaben sind die Aufrechterhaltung und Fortschreibung des Informationssicherheitsprozesses sowie die Bearbeitung von Informationssicherheitsvorfällen.

Das IST setzt sich wie folgt zusammen:

Informationssicherheitsbeauftragte/-r (ISB):

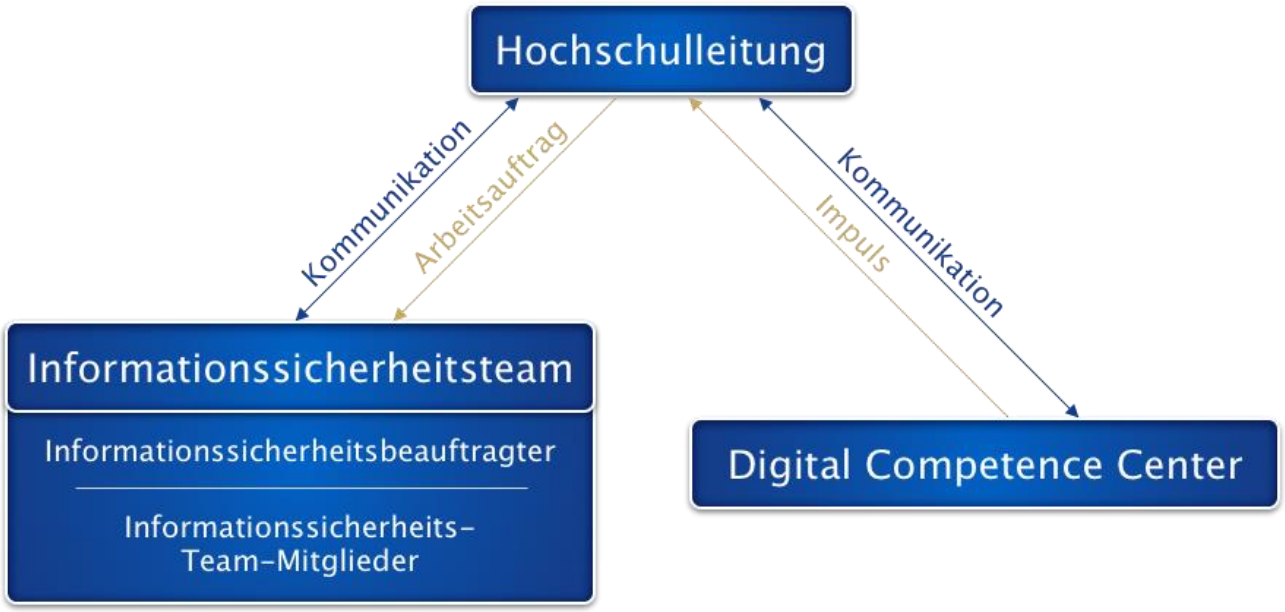
Die Präsidentin/Der Präsident benennt eine/-n Informationssicherheitsbeauftragte/-n, die/der über eine geeignete Fachkompetenz zur Informationssicherheit verfügt. Sie/Er ist für alle operativen Belange und Fragen der Informationssicherheit der Hochschule zuständig. Die/Der ISB berichtet in ihrer/seiner Funktion direkt an die Präsidentin/den Präsidenten, als verantwortliche/-n Vertreter/-in der Hochschulleitung.

Mitglieder Informationssicherheitsteam

Die Mitglieder unterstützten die/den ISB bei strategischen Entscheidungen wie z.B. der Bestimmung der Sicherheitsziele, der Sicherheitsstrategie und der Erstellung und Anpassung des Sicherheitskonzeptes. Die Mitglieder des IST werden durch die Hochschulleitung benannt.

Digital Competence Center (DCC)

Das DCC hat die Aufgabe, die „Digitale Agenda der TH Wildau“ zu definieren und der Hochschulleitung diese zur Freigabe zuzuarbeiten. Die Orientierung an einer digitalen Agenda soll das digitale Arbeiten auf allen Ebenen und in allen Bereichen der Hochschule durch den Einsatz einer zukunftsfähigen digitalen Infrastruktur und dazugehöriger Services gewährleisten. Das DCC wirkt als Impulsgeber bei der Fortschreibung des Informationssicherheitsprozesses.


Hochschulleitung
Kommunikation
Arbeitsauftrag
Impuls
Kommunikation
Informationssicherheitsteam
Informationssicherheitsbeauftragter
Informationssicherheits-
Team-Mitglieder
Digital Competence Center

Sicherheitsmaßnahmen

Für alle Prozesse, Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person entsprechend der Organisationsstruktur benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen festlegt. Dies dient der eindeutigen Nachverfolgbarkeit bei der Vergabe von Zugriffsberechtigungen.

Für alle verantwortlichen Funktionen sind Vertretungen zu benennen. Es muss durch Unterweisung und angemessene Dokumentation sichergestellt sein, dass Vertretungen ihre Aufgaben erfüllen können.

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

Auf allen IT-Systemen wird, soweit technisch möglich, ein geeigneter Schutz vor Schadsoftware 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 alle Angehörigen der Hochschule die festgelegten Maßnahmen durch eine sicherheitsbewusste Arbeitsweise und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Die Angehörigen der Hochschule informieren sich durch bereitgestellte Dokumentationen und nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Diese Informationen zu den Maßnahmen finden sich auf der Webseite im Bereich der Informationssicherheit[3] wieder. Die Hochschulleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Wenn Sicherheitsrisiken auftreten (bekannte oder drohende Angriffe), kann die Verfügbarkeit von Informationen entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten Hochschule ist der Schutz vor Schäden vorrangig.

Informationsverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass beeinträchtigte Prozesse oder Arbeitsabläufe kurzfristig wiederaufgenommen werden können, wenn Teile des operativen Datenbestandes verlorengehen oder offensichtlich fehlerhaft sind.

[3] https://www.th-wildau.de/informationssicherheit

Fortschreibung des Informationssicherheitsprozesses

Das Informationssicherheitsmanagementsystem der TH Wildau wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Angehörigen der Hochschule bekannt sind und ob sie umsetzbar und in den Hochschulablauf integrierbar sind.

Die Hochschulleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Alle Angehörigen der Hochschule sind angehalten, mögliche Verbesserungen oder Schwachstellen an das Informationssicherheitsteam oder den Informationssicherheitsbeauftragten weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Informationssicherheitstechnik zu halten.

Inkrafttreten

Diese Informationssicherheitsleitlinie für die Technische Hochschule Wildau tritt am Tag ihrer Veröffentlichung in den Amtlichen Mitteilungen in Kraft. Die vorliegende Informationssicherheitsleitlinie wurde von der Hochschulleitung am 06.11.2020 beschlossen. Sie tritt an die Stelle der Informationssicherheitsleitlinie vom 30.08.2017, Amtliche Mitteilung 45/2017.

Wildau, 18. Dezember 2020

gez. Prof. Dr. rer. nat. Ulrike Tippe
Präsidentin
Der Technischen Hochschule Wildau