Trier University
of Applied Sciences

HOCHSCHULE TRIER

Leitlinie zur Informationssicherheit

Hochschule Trier

Inhalt

Maßnahme:	Leitlinie gemäß BSI IT-Grundschutz ISMS 1.A3
Geltungsbereich:	Alle Einrichtungen der Hochschule
Verantwortlich:	Das Präsidium
Wiedervorlage:	Alle 5 Jahre
Zuletzt geändert:	09.03.2023

Einleitung

Die Hochschule Trier versteht sich als international ausgerichtete Hochschule mit regionalen Wurzeln. Zum Erreichen ihrer strategischen Ziele und der Erfüllung ihrer Aufgaben in Forschung, Lehre und Verwaltung spielen Informationen eine zentrale Rolle. Informationen bilden die Grundlage fast aller hochschulweiten Abläufe. Aufgabe der Informationssicherheit ist es, diese Informationen, ob in analoger oder digitaler Form, und die zu ihrer Verarbeitung und Speicherung erforderlichen Prozesse und Systeme zu schützen. Auf diese Weise trägt sie maßgeblich dazu bei, dass die Hochschule Trier ihrem gesetzlichen Auftrag und ihren Selbstverpflichtungen gerecht werden kann.

Die Informationssicherheit an der Hochschule Trier orientiert sich an der DSGVO sowie den jeweils aktuellen Richtlinien zum IT-Grundschutz, veröffentlicht im IT-Grundschutz-Kompendium[1] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und dem vom ZKI e.V. daraus abgeleiteten IT-Grundschutz Profil für Hochschulen[2].

Das Präsidium der Hochschule Trier bekennt sich zu den Zielsetzungen der Informationssicherheit und deren verantwortungsvollen Umsetzung. Die Leitlinie zur Informationssicherheit dokumentiert dieses Bekenntnis und formuliert den strategisch-organisatorischen Rahmen der Informationssicherheit an der Hochschule Trier**.**

Geltungsbereich

Die Leitlinie gilt für alle Personen und Institutionen, die IT-Infrastruktur, Netzwerke und daran angeschlossene IT-Systeme der Hochschule Trier an beliebigen Standorten der Hochschule Trier nutzen oder selbst IT-Systeme in diesem Umfeld betreiben.

Ziele

Die Maßnahmen zur Informationssicherheit sollen ein, auf einer Risikoanalyse basierendes, angemessenes Sicherheitsniveau gewährleisten, um Schaden von der Hochschule Trier abzuwenden. Um das angestrebte Sicherheitsniveau zu erreichen und die jeweils geltenden gesetzlichen und vertraglichen Regelungen zu erfüllen, werden folgende Ziele angestrebt:

Verfügbarkeit:

> Systeme, Anwendungen und Daten müssen den Berechtigten in jeder Situation wie vorgesehen zeitgerecht zur Verfügung stehen.

Vertraulichkeit:

> Der Zugriff und die Nutzung von Daten jeglicher Art darf ausschließlich durch berechtigte Personen in definierter und zulässiger Weise erfolgen.

Integrität:

> Die Unversehrtheit von Daten muss jederzeit gewahrt sein. Dies umfasst auch, dass Informationen und Daten nicht unerlaubt erstellt oder verändert werden können.

[1] BSI IT-Grundschutz-Kompendium (in der jeweils aktuellen Fassung, zuletzt abgerufen am 01.03.2023)
[2] IT-Grundschutz-Profil für Hochschulen (zuletzt abgerufen am 01.03.2023)

Strategie

Informationssicherheitsmanagement

Zum Erreichen der Sicherheitsziele wird ein Informationssicherheitsmanagementsystem (ISMS) etabliert, welches Organisationsstrukturen und Prozesse definiert, die kontinuierlich überwacht, evaluiert und den aktuellen Erfordernissen angepasst werden. Hierzu sind ein lückenloses Asset-Management und geeignete Methoden des Monitorings erforderlich.

Das ISMS bildet den Kern der Sicherheitsstrategie und beinhaltet insbesondere folgende Komponenten:

Sensibilisierung

Die Hochschulmitglieder werden durch geeignete Maßnahmen in die Lage versetzt, den Stellenwert der Informationssicherheit im Rahmen ihrer Tätigkeit nachzuvollziehen, die Notwendigkeit von Maßnahmen zu verstehen und ihr eigenes Handeln an den allgemeinen Sicherheitszielen auszurichten.

Risikomanagement

Das operative Risikomanagement umfasst den Regelprozess aus Identifikation von Risiken, Einschätzung und Bewertung von Risiken, Behandlung von Risiken, Überwachung von Risiken und Risikokommunikation die Informationssicherheit betreffend. Aus der Risikoanalyse erfolgt in Absprache mit dem Präsidium die Auswahl und Umsetzung geeigneter Maßnahmen zur Behandlung beziehungsweise Minimierung dieser Risiken. Diese Maßnahmen werden im Konzept zur Informationssicherheit dokumentiert, welches jährlich überprüft wird.

Besondere organisatorische Maßnahmen sind die zu veröffentlichenden Richtlinien zur Informationssicherheit, die Vorgaben zum Umgang mit bestimmten Risiken machen. Sie sind verbindlich und werden jährlich überprüft.

Vorfallmanagement

Für die Behandlung von sicherheitsrelevanten Vorkommnissen werden Verantwortlichkeiten und Vorgehensweisen festgelegt. Notfallkonzepte und -pläne sollen die Wiederaufnahme bzw. Weiterführung des Geschäftsbetriebs auch in Not- und Krisenfällen unter Wahrung der Informationssicherheit gewährleisten. Dazu gehört auch die Festlegung eines Krisenmanagement-Teams.

Beteiligte und deren Aufgaben

Präsidium

Die Gesamtverantwortung für die Informationssicherheit liegt beim Präsidium der Hochschule Trier. Es stellt notwendige Ressourcen bereit, verabschiedet die vorliegende Leitlinie zur Informationssicherheit und veranlasst deren Überprüfung nach spätestens 5 Jahren.

Beauftragte Person für Informationssicherheit (ISB)

Das Präsidium bestellt eine Beauftragte Person für Informationssicherheit (ISB) an der Hochschule Trier, die als qualifizierte Fachkraft verantwortlich für den Bereich Informationssicherheit ist. Der Fokus liegt dabei auf einer hochschulweiten, ganzheitlichen Perspektive, die die Verwaltung, Forschung und Lehre umfasst. Die beauftragte Person für Informationssicherheit ist in Fragen der Informationssicherheit nur an Weisungen des Präsidiums gebunden.

In ihre Zuständigkeit fallen die Konzeption, Steuerung, Dokumentation und Weiterentwicklung des ISMS sowie darüber hinaus die Risikoanalyse, Untersuchung von Sicherheitsvorfälle und die Berichte

an das Präsidium zum Stand der Informationssicherheit. Die beauftragte Person verantwortet die Erstellung des Konzepts zur Informationssicherheit und daraus abgeleiteter Richtlinien gemeinsam mit allen am Sicherheitsprozess Beteiligten. Zur Erfüllung dieser Aufgaben werden die notwendigen Ressourcen und Informationen zur Verfügung gestellt.

In Abstimmung mit dem Präsidium besteht Weisungsrecht in kritischen Fragen der Informationssicherheit.

Sofern ein Team Informationssicherheit etabliert wird, können auch mehrere Personen zu Informationssicherheitsbeauftragten bestellt werden.

Senatsbeauftragte Person für Informationssicherheit (SBIS)

Die senatsbeauftragte Person für die Informationssicherheit wird vom Senat ernannt. Die Aufgaben umfassen in Abstimmung mit der oder dem ISB die strategische Weiterentwicklung des ISMS, die Risikoanalyse und die Beratung zu Fragen der Informationssicherheit. Die oder der SBIS gehört dem Team Informationssicherheit an.

Krisenmanagement-Team

Das Krisenmanagement-Team steuert und koordiniert alle Maßnahmen bei Sicherheitsvorfällen, die die Informationssicherheit betreffen. Das Kernteam besteht aus ISB, SBIS, DSB und der Leitung der zentralen Rechenzentren. Bei Bedarf wird das Team durch Personen des Präsidiums und ggf. Personen aus betroffenen Einrichtungen ergänzt.

Leitung der zentralen Rechenzentren

Die Leitung der zentralen Rechenzentren ist verantwortlich für die Sicherheit der IT-Infrastruktur und der zentral betriebenen und betreuten IT-Systeme und sorgt für die Umsetzung der Sicherheitsmaßnahmen.

Verantwortliche für IT-Systeme

Die Verantwortlichkeit für Informationssicherheit folgt grundsätzlich den Zuständigkeiten für IT-Systeme, d. h. jede Person, die ein IT-System im Netzwerk der Hochschule Trier betreibt, ist über die gesamte Lebenszeit des Systems für den ordnungsgemäßen und sicheren Betrieb bis zur Stilllegung und fachgerechten Entsorgung verantwortlich.

Beauftragte Person für Datenschutz (DSB)

Die beauftragte Person für Datenschutz beurteilt die Maßnahmen zur Informationssicherheit bezüglich des Datenschutzes. Sie ist bei Sicherheitsvorfällen, die personenbezogene oder sonstige sensible Daten betreffen, einzubeziehen.

Rechte und Pflichten

Mitwirkung

Die Nutzenden der IT-Infrastruktur der Hochschule Trier gehen täglich mit großen Mengen an Informationen um. Damit der Schutz dieser Informationen gelingen kann, ist die Mitwirkung all dieser Personen zwingend erforderlich. Sie schützen Informationen, Prozesse und Systeme entsprechend ihres Wertes nach bestem Wissen und Vermögen.

Kommunikation

Bei Informationssicherheitsrisiken und –vorfällen ist in jedem Fall die oder der ISB sowie die oder der unmittelbar Vorgesetzte unverzüglich zu informieren. Die Kommunikation mit Dritten außerhalb der Hochschule erfolgt immer durch ISB, DSB oder das Präsidium.

Bei der Konzeption, Einführung und Umgestaltung informationsverarbeitender Systeme und Prozesse ist die oder der ISB rechtzeitig einzubinden.

Gefahrenintervention

Bei Gefahr im Verzug sind die oder der ISB und die unmittelbar Verantwortlichen für die betroffenen IT-Systeme oder Prozesse berechtigt, unmittelbar notwendige Abwehrmaßnahmen vorzunehmen. Bei den zu treffenden Maßnahmen ist der Grundsatz der Verhältnismäßigkeit der Mittel zu wahren. Die Maßnahmen sollten so erfolgen, dass betroffene Nutzerinnen und Nutzer - wenn irgend möglich - bereits vorher in Kenntnis gesetzt werden. Abhängig von der Art des Vorfalls sind im Nachgang alle relevanten Stellen zu informieren (Präsidium, DSB, ISB, Personalvertretung).

Inkrafttreten

Diese Leitlinie zur Informationssicherheit für die Hochschule Trier tritt mit ihrer Veröffentlichung am 14.04.2023 in Kraft. Sie gilt bis auf Widerruf. Der Gesamtpersonalrat hat am 03.04.2023 zugestimmt.

Glossar

BSI	Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de)
DSB	Datenschutzbeauftragte
DSGVO	Datenschutz-Grundverordnung (dsgvo-gesetz.de)
ISB	Informationssicherheitsbeauftragte
ISMS	Informationssicherheitsmanagementsystem
SBIS	Senatsbeauftragter für Datenschutz und Informationssicherheit
ZKI e.V.	Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e.V. (zki.de)