Fachhochschule Potsdam
University of
Applied Sciences

Leitlinie zur Informations-sicherheit

Fachhochschule Potsdam

Dokumentenname:	A_02_Leitlinie_Informationssicherheit
Version/ Änderungsdatum:	Version 1.1 / 17.05.21
Geltungsbereich:	Alle Einrichtungen der FH Potsdam
Verantwortlich:	Hochschulleitung
Revision:	Jährlich

Inhaltsverzeichnis

1. Präambel

Die Leitlinie zur Informationssicherheit beschreibt die grundlegenden Ziele und Rahmenvorgaben für die Informationssicherheit der FH Potsdam und welche Bedeutung diese für die FH Potsdam hat.

Informationen sind das Kerngeschäft der FH Potsdam, wobei Forschung Informationen generiert. So sind Informationen zum Beispiel Forschungsdaten, Ergebnisse weltweiter Kommunikation oder die Zusammenfassung von Recherchen. Weiterhin werden in der Lehre und Weiterbildung Informationen vermittelt. Dies erfolgt zum Beispiel über e-Learning, Videokonferenzen, (digitale) Bibliotheksysteme genauso wie in Lehrformaten, welche ohne den Einsatz von Informationstechnologie durchgeführt werden. Auch spielen Informationen bei der Administration der Hochschule eine zentrale Rolle. Sie werden zur Verwaltung von Personal-, Studierenden- und Prüfungsdaten, sowie zur Finanzsteuerung eingesetzt und erstellt. Informationen kommen an der FH Potsdam in digitaler und analoger Form zum Beispiel in Ausdrucken, handschriftlichen Arbeiten und Vermerken, Büchern oder Printmedien vor. Sie werden in einem breiten Spektrum erstellt, verbreitet, bearbeitet und gelöscht.

Die Heterogenität, also Verschiedenartigkeit, der eingesetzten Systeme und Komponenten im IT-Umfeld und Nutzer*innen sowie der zu verarbeitenden Informationen, die in der Vielzahl der aufgeführten Einsatzfelder begründet liegt, bietet ein hochinteressantes und breites Angriffsziel für sicherheitskritische Angriffe von innen und außen. Neben der Abwehr dieser Angriffe auf Daten und Systeme ist die Aufrechterhaltung des Geschäftsbetriebs, also der Lehre und Forschung sowie der Administration und Organisation, ein wesentliches Ziel der Informationssicherheit.

Informationssicherheit ist für die FH Potsdam unverzichtbar. Sie ist Voraussetzung für den Erfolg und Gesetzeskonformität in Lehre, Forschung und Weiterbildung. Die Mitglieder und Angehörigen der Hochschule sind dabei gleichzeitig Betroffene und Akteure der Informationsverarbeitung.

Die Leitlinie zur Informationssicherheit der FH Potsdam beschreibt allgemeinverständlich, was Informationssicherheit ist und welche Bedeutung sie für die FH Potsdam hat.

Die Leitlinie zur Informationssicherheit ist Bestandteil eines hierarchisch abgestuften Regelwerks und bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte sowie Regelungen und Dienstanweisungen zur Informationssicherheit.

2. Geltungsbereich

Diese Leitlinie gilt für alle Mitglieder und Angehörigen der FH Potsdam sowie in der Zusammenarbeit ebenfalls für alle externen Geschäfts- und Kooperationspartner, soweit diese entsprechend gebunden sind. Sie sind unabhängig von ihrer Rolle und Stellung in der Hochschule aufgefordert, sich jederzeit für die Wahrung der Informationssicherheit und die Erreichung der Sicherheitsziele einzusetzen.

Alle Mitarbeitenden und Angehörige der FH Potsdam richten sich bei der Zusammenarbeit untereinander und mit Dritten, die mittelbar oder unmittelbar an das Netz der Hochschule angeschlossen sind, nach dieser Leitlinie.

3. Sicherheitsziele

Aufgabe und Ziel der Informationssicherheit ist der angemessene Schutz der drei Grundwerte:

- **Integrität**
  Mit diesem Begriff wird die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen bezeichnet. Bei intakter Integrität sind Daten vollständig und unverändert. Eventuell zugehörige Attribute wurden nicht unerlaubt manipuliert.

- **Verfügbarkeit**
  Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen, IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

- **Vertraulichkeit**
  Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen, aber auch der Zutritt zu Räumlichkeiten dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

4. Sicherheitsstrategie

Zum Erreichen der Sicherheitsziele wird ein Informationssicherheitsmanagementsystem (ISMS), orientiert an der ISO 27001 auf Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), als kontinuierlicher Informationssicherheitsprozess an der FH Potsdam festgelegt, umgesetzt, durchgeführt, überwacht, überprüft, instandgehalten und verbessert. Verantwortlich für Betrieb und Weiterentwicklung des ISMS ist der Informationssicherheitsbeauftragte.

Der Aufbau eines Informationssicherheitsmanagementsystems bildet den Kern der Sicherheitsstrategie und beinhaltet insbesondere folgende Komponenten:

- **Sensibilisierung**
  Die Beschäftigten werden durch Informationsveranstaltungen und Schulungen 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 Sicherheitszielen auszurichten.

- **Risikoanalyse**
  Im Rahmen einer ganzheitlichen Analyse der bestehenden Informationsverarbeitung, technisch wie konventionell, werden alle Elemente bezüglich ihrer Gefährdungen und der damit verbundenen Schadenshöhe bewertet. Darauf aufbauend erfolgten die Auswahl und Umsetzung spezifischer Maßnahmen zur Behandlung dieser Risiken.

- **Vorfallmanagement**
  Für die Behandlung von sicherheitsrelevanten Vorkommnissen werden Verantwortlichkeiten und Vorgehensweisen festgelegt.

- **Notfallmanagement**
  Der Wiederanlauf und die Wiederherstellung des Geschäftsbetriebs in Not- und Krisenfällen werden durch Notfallkonzepte und -pläne gewährleistet. Dabei wird die Informationssicherheit auch in solchen Ausnahmesituationen sichergestellt.

5. Sicherheitsmaßnahmen

Durch die Umsetzung von Sicherheitsmaßnahmen soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheit geboten wird, um Informationswerte und Daten zu schützen und deren Verfügbarkeit zu gewährleisten. Die Schutzmaßnahmen orientieren sich an folgenden Vorgaben:

- Informationen und Systeme werden bezüglich ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Ausfallzeiten toleriert werden können. Ausfallzeiten, die zu größeren Arbeitsverzögerungen oder Fristversäumnissen führen können, sollen durch entsprechende Maßnahmen vermieden werden.

- Die Anforderungen an Integrität und Vertraulichkeit orientieren sich an der Gesetzeskonformität.

- Für alle Prozesse, Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen festlegt.

- Für alle verantwortlichen Funktionen werden Vertretungen eingerichtet. Es muss durch Unterweisung und angemessene Dokumentation sichergestellt sein, dass Vertreter deren 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 restriktives Berechtigungskonzept geschützt.

- Auf allen IT-Systemen wird, soweit technisch möglich, ein geeigneter Schutz vor Schadsoftware eingesetzt. Zugänge zum Hochschulnetz werden durch eine geeignete Firewall sowie ein für den Einsatzzweck angepasstes Regelwerk gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden können.

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

- ISMS-Maßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen stehen. Schadensfälle mit hohen finanziellen oder immateriellen Auswirkungen müssen verhindert werden.

  Die konkreten Sicherheitsmaßnahmen für die einzelnen Informationen und Informationsklassen werden in einem auf den jeweiligen Schutzbedarf angepasstem Informationssicherheitskonzept erarbeitet.

6. Verantwortung und Organisationsstruktur

Um die Informationssicherheit an der FH zu gewährleisten wird eine Organisationstruktur an der FH Potsdam etabliert. Diese wird in folgenden Rollen und Verantwortlichkeiten definiert.

- **Hochschulleitung**
  Die Hochschulleitung der FH Potsdam trägt die Gesamtverantwortung für die Informationssicherheit. Sie erlässt verbindliche Regeln zur Informationssicherheit für die FH Potsdam und gibt sie den Mitarbeitenden und Studierenden bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher.

- **Informationssicherheitsbeauftragte/n (ISB)**
  Die beauftragte Person für Informationssicherheit ist für alle operativen Belange und Fragen der Informationssicherheit der Hochschule zuständig. Die/der ISB berichtet in seiner Funktion direkt an die Hochschulleitung.

- **Datenschutzbeauftragter/n (DSB)**
  Die Gewährleistung des Schutzes des Grundrechts auf informationelle Selbstbestimmung nach dem Datenschutzrecht hat eine andere Aufgabenstellung als die Informationssicherheit und ist daher nicht Gegenstand dieser Richtlinie. Jedoch arbeiten ISB und DSB eng zusammen, soweit sie gemeinsame, insbesondere technische Schutzziele teilen. Die/der DSB wirkt beratend am Informationssicherheitsmanagement in Belangen des Datenschutzes mit.

- **Informationssicherheitsmanagement-Team (ISMT)**
  Die Hochschule richtet ein Informationssicherheitsmanagement-Team (ISMT) ein. Das ISMT unterstützt den ISB bei strategischen Entscheidungen wie z. B. der Bestimmung der Sicherheitsziele, der Sicherheitsstrategie, der Erstellung und der Anpassung des Sicherheitskonzeptes. Das Team setzt sich zusammen aus der Hochschulleitung, dem/der Informationssicherheitsbeauftragten/m, dem/der Datenschutzbeauftragten/m, der Leitung-/ Koordination für IT-Infrastruktur.

  Mitglieder der jeweils zuständigen Personalvertretungen oder betroffenen Fachanwendungen und Fachverfahren werden eingeladen, wenn dies im Sinne einer vertrauensvollen Zusammenarbeit oder aus personalvertretungsrechtlichen Gründen angezeigt ist.

7. Aktualisierung der Leitlinie

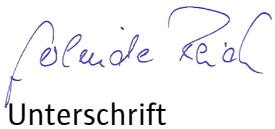
Um das definierte Sicherheitsniveau der FH Potsdam aufrecht zu erhalten, ist eine fortlaufende Kontrolle und Verbesserung der implementierten Sicherheitsmaßnahmen, Dokumente und des festgelegten Informationssicherheitsprozesses zwingend erforderlich.

Im Rahmen des Informationssicherheitsprozesses wird diese Leitlinie regelmäßig auf ihre Aktualität geprüft und im Bedarfsfall durch den Informationssicherheitsbeauftragen an die geänderten Anforderungen angepasst und aktualisiert.

8. Inkrafttreten und Veröffentlichung

Diese Informationssicherheitsleitlinie tritt am Tag nach ihrer Veröffentlichung in Kraft. Sie wird allen Hochschulangehörigen dauerhaft und in aktualisierter Form zur Verfügung gestellt.

Potsdam, 17.05.2021



Unterschrift

Gerlinde Reich
Kanzlerin