Leitlinie zur Informationssicherheit der Universität Potsdam

Vom 10. Mai 2023

Das Präsidium der Universität Potsdam hat am 5. April 2023 folgende Leitlinie zur Informationssicherheit verabschiedet, die am 10. Mai 2023 von Senat zustimmend zur Kenntnis genommen wurde:

Präambel

Die Universität Potsdam verarbeitet im Rahmen ihrer Forschungs-, Lehr-, Transfer- und Verwaltungstätigkeiten eine Vielzahl von Informationen in digitaler und analoger Form. Dabei fallen an verschiedenen Stellen der Hochschule personenbezogene oder andersgeartete sensible Daten an, die einen hohen Schutzbedarf aufweisen und somit vor einem unbefugten Zugriff durch Dritte besonders zu schützen sind.

Die Heterogenität der Informationsverarbeitungssysteme und -verfahren bietet ein breites Angriffsziel für sicherheitskritische Angriffe von innen und außen. Neben dem Schutz von Daten ist zur Aufrechterhaltung des Hochschulbetriebs auch die Abwehr von Angriffen auf zentrale und dezentrale IT-Systeme von großer Bedeutung.

Informationssicherheit spielt eine Schlüsselrolle für die Aufgabenerfüllung innerhalb der Universität Potsdam. Die Leitlinie zur Informationssicherheit stellt die Sicherheitsstrategie, die Sicherheitsorganisation und die Sicherheitsziele in übersichtlicher und allgemeinverständlicher Form dar. Die Leitlinie ist Bestandteil eines hierarchisch abgestuften Regelwerks und bildet die Grundlage für die Erstellung weiterer, auch fachspezifischer Richtlinien, Informationssicherheitskonzepte sowie Regelungen und Dienstanweisungen zur Informationssicherheit.

Geltungsbereich

Diese Leitlinie gilt für alle Mitglieder und Angehörige der Universität Potsdam sowie für alle Hochschulexternen, die IT-Verfahren, IT-Dienste oder sonstige informationsverarbeitende Verfahren der Universität benutzen. Ausnahmen für Externe bedürfen der schriftlichen Zustimmung der Hochschulleitung oder einer berechtigten Vertretung sowie der Zustimmung der/des Informationssicherheitsbeauftragen. Die Ausnahmen sind zeitlich zu begrenzen und mindestens jährlich zu prüfen.

Grundsätze und Ziele der Informationssicherheit

Es gelten die allgemeinen Schutzziele der Informationssicherheit: **Verfügbarkeit**, **Integrität** und **Vertraulichkeit**. Für die Universität Potsdam ergeben sich daraus konkret folgende Ziele:

- Zuverlässige Unterstützung der Geschäftsprozesse durch die IT und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb Hochschule,
- Realisierung sicherer und vertrauenswürdiger Verarbeitungsverfahren,
- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Erhalt bzw. Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen,
- Gewährleistung des informationellen Selbstbestimmungsrechts der betroffenen Person bei der Verarbeitung personenbezogener Daten,
- Einführung eines kontinuierlichen Verbesserungsprozesses,
- Reduzierung der im Schadensfall entstehenden Kosten sowie
- Wahrung besonderer Geschäftsgeheimnisse und Forschungsergebnisse.

Neben den allgemeinen Schutzzielen können für jeden Fachbereich weitere bzw. angepasste Schutzziele aufgestellt werden.

Sicherheitsmaßnahmen

Ziele und Aufwand von Sicherheitsmaßnahmen werden bestimmt durch die Bedeutung der Verarbeitungsprozesse für die jeweiligen Bearbeitungsfälle. Neben der Beachtung gesetzlicher Anforderungen müssen Sicherheitsmaßnahmen zugleich auch immer auf Verhältnismäßigkeit geprüft werden, d.h. die Maßnahmen müssen wirtschaftlich gesehen in einem vertretbaren Verhältnis zum Wert der geschützten Informationen stehen. Sollten die gestellten Sicherheitsanforderungen nicht finanzierbar sein, müssen die Sicherheitsanforderungen, aber auch die Arbeitsprozesse und die angewendeten IT-Verfahren grundsätzlich überdacht werden.
Bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen ist darauf zu achten, dass die Arbeitsprozesse möglichst wenig durch die gewählten Sicherheitsmaßnahmen beeinträchtigt werden.
Alle Personen aus dem Geltungsbereich der Universität Potsdam sind sich ihrer Verantwortung für die Informationssicherheit bewusst und haben diese Sicherheitsleitlinie zu unterstützen. Informationssicherheit betrifft ohne Ausnahme alle Hochschulangehörigen. Jede einzelne Person kann durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden zu vermeiden und zum Erfolg der Hochschule beizutragen. Sensibilisierung für Informationssicherheit und fachliche Schulungen der

Mitarbeitenden sind daher eine Grundvoraussetzung für Informationssicherheit. Mitarbeitende 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 anwendende Person transparent und verständlich sein, sofern dadurch kein Sicherheitsrisiko entsteht.

Verantwortlichkeiten

Die Hochschulleitung trägt die Gesamtverantwortung für die Informationssicherheit. Im Rahmen dieser Gesamtverantwortung delegiert sie Entscheidungsbefugnisse für gesamtstrategische Maßnahmen an die/den Chief Information Officer (CIO), dem das Zentrum für Informationstechnologie und Medienmanagement (ZIM) direkt unterstellt ist, sowie die Verantwortlichkeiten für operative Maßnahmen an die Leitungen der Fakultäten, der zentralen Verwaltungseinheiten und der zentralen und sonstigen Einrichtungen. Allen Organisationsebenen der Hochschule obliegt die operative Verantwortung für die Informationssicherheit in ihren jeweiligen Bereichen.
Zur Erreichung der Informationssicherheitsziele wird eine Informationssicherheitsbeauftragte oder ein Informationssicherheitsbeauftragter von der Hochschulleitung benannt. Die bzw. der Informationssicherheitsbeauftragte berät die Hochschulleitung und benennt Zuständigkeiten bei der Planung und Umsetzung der Informationssicherheit innerhalb der Hochschule. Sie bzw. er berichtet in ihrer/seiner Funktion anlassbezogen, mindestens jedoch einmal jährlich, unmittelbar an die Hochschulleitung.

Informationssicherheitsorganisation

Die bzw. der Informationssicherheitsbeauftragte darf keine Interessenkonflikte mit strategischen Zielen der Leitungsebene und der IT-Leitung haben. Zur Informationssicherheitsorganisation zählen neben der bzw. dem Informationssicherheitsbeauftragten, die bzw. der Datenschutzbeauftragte sowie die Leitung des ZIM. Anlassbezogen können auch die Personalvertretung, andere Stabsstellen sowie ZIM-Teamleitungen hinzugezogen werden.
Der bzw. dem Informationssicherheitsbeauftragten und allen mit der operativen Umsetzung befassten Beschäftigten werden ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, sich zu informieren und die von der Hochschulleitung festgelegten Sicherheitsziele zu erreichen.
Die bzw. der Informationssicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für die Datenschutzbeauftragte bzw. den Datenschutzbeauftragten.

Umsetzung

Diese Leitlinie bildet die Basis zur Erstellung weiterer Richtlinien, Informationssicherheitskonzepte sowie detaillierter Prozesse und Regelungen zur Informationssicherheit. Die Umsetzung erfolgt im Rahmen eines Informationssicherheitsmanagementprozesses. Die Einhaltung von Vorgaben weiterer Regelungen sind für die jeweils adressierten Zielgruppen verpflichtend.

Kontinuierliche Verbesserung

Diese Sicherheitsleitlinie sowie das Informationssicherheitskonzept werden regelmäßig, spätestens jedoch im Abstand von einem Jahr auf ihre Aktualität und Wirksamkeit geprüft und angepasst.
Die Hochschulleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Alle Personen aus dem Geltungsbereich der Universität Potsdam sind angehalten, mögliche Verbesserungen oder Schwachstellen an die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten weiterzugeben.

Inkrafttreten und Veröffentlichung

Diese Benutzungsordnung tritt einen Tag nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Universität Potsdam in Kraft.