

Leitlinie zur Informationssicherheit der Universität Paderborn

PRÄAMBEL

Der Hochschulbetrieb erfordert zunehmend die Verwendung von Verfahren und Abläufen, die sich auf Möglichkeiten der Informations- und Kommunikationstechnik (IT) stützen. Sie sind somit eine zentrale Grundlage für die Leistungsfähigkeit der Universität Paderborn als Universität der Informationsgesellschaft. Unter diesen Bedingungen kommt der „Sicherheit in der Informationstechnik“ („IT-Sicherheit“) eine grundsätzliche und strategische Bedeutung zu. Auf Grund der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten, der Heterogenität der IT-Landschaft und verteilten Verantwortung, muss ein kontinuierlicher IT-Sicherheitsprozess realisiert werden, der den besonderen Bedingungen einer Hochschule gerecht wird.

Die Entwicklung und Fortschreibung des IT-Sicherheitsprozess soll sich einerseits an den gesetzlich festgelegten Aufgaben der Universitäten sowie an ihrem Mandat zur Wahrung der akademischen Freiheit orientieren, andererseits soll sie keinen Selbstzweck erfüllen, sondern auf Grund von gesetzlichen Auflagen, Anforderungen der Universität Paderborn sowie Belangen von Anwenderinnen und Anwendern eine risikogerechte Bewertung von Gefährdungen vornehmen sowie entsprechende Maßnahmen einleiten.

Die vorliegende Leitlinie zur Informationssicherheit und das ergänzende Regelwerk zur Informationssicherheit dienen dazu, diesen Anspruch umzusetzen. Das Präsidium hat die Leitlinie beschlossen und unterstützt die erforderlichen Maßnahmen zur Realisierung der Informationssicherheit.

ZIELE UND ADRESSATENKREIS

Diese Leitlinie regelt die Verantwortung und die Zuständigkeiten sowie die Zusammenarbeit im hochschulweiten IT-Sicherheitsprozess. Es ist ihr Ziel nicht nur die existierenden gesetzlichen Auflagen zu erfüllen, sondern auch die in der Hochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen vor Missbrauch zu schützen.

Sie ist an alle Organisationseinheiten, Mitglieder und Angehörige der Universität Paderborn sowie an Dritte gerichtet, die IT-Systeme und IT-Verfahren benutzen oder betreiben.

LEITSÄTZE

Die Universität erfüllt die gesetzlichen Regelungen und vertraglichen Auflagen im Bereich der Informationssicherheit und des Datenschutzes sowie die Grundsätze der guten wissenschaftlichen Praxis. Sie orientiert sich insbesondere an den Schutzziele der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz beim Umgang mit personenbezogenen Daten.

Als zusätzliche Prinzipien der Informationssicherheit sind für die Universität Paderborn festgelegt

- **Wohlorganisiertheit:** Für alle IT-Systeme und IT-Verfahren gibt es klare Verantwortlichkeiten

- **Informiertheit:** Alle Anwenderinnen und Anwender von IT-Systemen und IT-Verfahren sollen sich der für sie wesentlichen Sicherheitsrisiken und deren Abwehrmaßnahmen bewusst sein.
- **Zurechenbarkeit:** Jede von vernetzten Rechnern der Universität Paderborn ausgehende Aktivität soll einer Person zugeordnet werden können.
- **Aktualität:** Die eingesetzten IT-Systeme und IT-Verfahren sollen den jeweils aktuellen Sicherheitsempfehlungen einschlägiger Institutionen entsprechen.
- **Angemessenheit:** Alle Maßnahmen sind mit Augenmaß und in Hinblick auf die Gefährdungen und Risiken sowie ihr Kosten-Nutzen-Verhältnis zu wählen.
- **Wahrung eines permanenten Regelkreislaufes:** Die Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen wird regelmäßig überprüft. Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert.
- **Recht auf informationelle Selbstbestimmung:** Die Universität unterstützt aktiv das Recht auf informationelle Selbstbestimmung und ist bestrebt die Erhebung, Speicherung und Nutzung personenbezogener Daten auf das Notwendige zu beschränken (Minimalität).

VERANTWORTLICHKEITEN

Die Leitung der Universität trägt die Gesamtverantwortung für die Informationssicherheit an der Universität Paderborn. Diese wird fachlich durch den Lenkungskreis für Informationssicherheit (LIS) wahrgenommen.

Die Verantwortung für die IT-Sicherheit jeder Organisationseinheit oder Einrichtung liegt bei der jeweiligen Leitung. Sie kann fachlich durch einen IT-Verantwortlichen wahrgenommen werden.

Falls externe Dienstleister beauftragt werden sind diese bei Aufnahme einer Vertragsbeziehung über entsprechende Passagen im Regelwerk zur Informationssicherheit zu informieren und schriftlich auf dessen Einhaltung zu verpflichten.

Alle Anwenderinnen und Anwender tragen die Verantwortung, bestimmungsgemäß und sachgerecht mit den von ihnen genutzten IT-Systemen, IT-Verfahren und Informationen umzugehen.

Die Finanzierung von Maßnahmen zur Informationssicherheit wird von den jeweiligen Verantwortlichen sichergestellt. Bei der Einführung neuer Verfahren ist die Sicherheit bereits bei der Planung zu berücksichtigen.

ORGANISATIONSSTRUKTUR

Zur Gestaltung des Informationssicherheitsprozesses an der Universität Paderborn wird die im Folgenden beschriebene Organisationsstruktur festgelegt. Sie besteht aus dem Lenkungskreis für Informationssicherheit, dem IT-Sicherheitsbeauftragten sowie den IT-Verantwortlichen und dem Computer Notfallteam.

Lenkungskreis für Informationssicherheit (LIS)

Der Lenkungskreis für Informationssicherheit (LIS) steuert im Auftrag des Präsidiums den IT-Sicherheitsprozess an der Universität Paderborn.

Er erarbeitet und empfiehlt in Zusammenarbeit mit den Verantwortlichen im Bereich Informationssicherheit strategische Empfehlungen und Maßnahmen wie diese Leitlinie und das Regelwerk zur Informationssicherheit und überprüft ihre Umsetzung.

Er berät das Präsidium im Bereich Informationssicherheit und empfiehlt und verantwortet hochschulweite Projekte in diesem Bereich.

Er nimmt die jährlichen Berichte der IT-Verantwortlichen im Bereich Informationssicherheit entgegen und berichtet einmal jährlich dem Präsidium zum Stand der Umsetzung der Informationssicherheit an der Universität Paderborn.

Er wählt aus seiner Mitte einen Ansprechpartner für Informationssicherheit, den IT-Sicherheitsbeauftragten der Universität Paderborn.

Zum Lenkungskreis zählen

- der CIO oder ein anderer Beauftragte oder eine Beauftragte des Präsidiums
- die/der behördliche Datenschutzbeauftragte
- jeweils eine Vertreterin oder ein Vertreter der Personalräte
- jeweils eine Vertreterin oder ein Vertreter der zentralen Organisationseinheiten, die hochschulweite IT-Systeme und IT-Verfahren verantworten, derzeit die Universitätsverwaltung, die Universitätsbibliothek, das Zentrum für Informations- und Medientechnologien (IMT)
- eine vom Präsidium benannte fachkundige Wissenschaftlerin oder ein vom Präsidium benannter fachkundiger Wissenschaftler
- die IT-Verantwortlichen der Fakultäten
- eine fachkundige Vertreterin oder ein fachkundiger Vertreter aus der Studierendenschaft (nach der Einführungsphase)

Das Präsidium sowie der LIS können weitere Teilnehmende zur Beratung hinzuziehen.

IT-Sicherheitsbeauftragter der Universität

Die/Der IT-Sicherheitsbeauftragte ist die zentrale Ansprechperson zu Fragen der Informationssicherheit an der Universität Paderborn.

Sie/Er koordiniert die Umsetzung der vom LIS empfohlenen Maßnahmen und verantwortet die Weiterentwicklung und Veröffentlichung des Regelwerks für Informationssicherheit.

Sie/Er berät die Organisationseinheiten, die Datenschutzbeauftragte oder den Datenschutzbeauftragten und organisiert Schulungs- und Sensibilisierungsmaßnahmen.

IT-Verantwortliche

Jede Organisationseinheit (Fakultäten, zentrale wissenschaftliche Einrichtungen, ZV, zentrale Betriebseinheiten) bestellt eine Person, die auf Grund ihrer Stellung, ihrer beruflichen Erfahrung und ihres Wissens qualifiziert ist, die Aufgaben einer /eines IT-Verantwortlichen zu übernehmen. Die Tätigkeit kann auch bereichsübergreifend wahrgenommen werden. Die Benennung ist zu dokumentieren und dem LIS anzuzeigen. Falls kein IT-Verantwortlicher bestellt wird, nimmt die Leitung der Organisationseinheit diese Funktion wahr. Entsprechende personelle Ressourcen müssen von den Organisationseinheiten zur Verfügung gestellt werden.

Die IT-Verantwortlichen sind zugleich Ansprechpartner für Informationssicherheit und tragen Sorge für die Weiterentwicklung von Maßnahmen sowie die Umsetzung der im IT-Sicherheitsprozess erarbeiteten Vorgaben. Sie informieren und berichten dem IT-Sicherheitsbeauftragten über Sicherheitsvorfälle in ihrem Verantwortungsbereich. Vorfälle mit Bezug auf personenbezogene Daten sind unverzüglich und unmittelbar dem IT-Sicherheitsbeauftragten anzuzeigen.

Computer Notfallteam

Das Computer Notfallteam der Universität Paderborn berät und unterstützt Organisationseinheiten bei der technischen Eingrenzung und Behebung von Angriffen, Störungen und Problemen durch die die Informationssicherheit verletzt wird oder verletzt werden kann. Das Notfallteam ist dem Störungsmanagement des IMT angegliedert. Es wird bei hochschulweiten Sicherheitsvorfällen in Absprache mit dem IT-Sicherheitsbeauftragten und dem Störungsmanager des IMT tätig und berichtet dem LIS über Sicherheitsvorfälle und deren Behebung.

REGELWERK ZUR INFORMATIONSSICHERHEIT

Diese Leitlinie bestimmt die Grundzüge der Informationssicherheit an der Universität Paderborn. Sie wird ergänzt durch ein Regelwerk zur Informationssicherheit, in dem grundlegende allgemeine Regelungen und Hinweise wie beispielsweise physikalische Sicherheit, Zutritts- und Zugangskontrolle, Rollen- und Rechte, Update- und Patchverpflichtung festgeschrieben werden. Zusätzlich werden detaillierte Maßnahmen und Policies beispielsweise für Organisationseinheiten oder Klassen von IT-Verfahren oder IT-Systemen beschrieben.