BERGISCHE
UNIVERSITÄT
WUPPERTAL

AMTLICHE MITTEILUNGEN

Verkündungsblatt der Bergischen Universität Wuppertal
Herausgegeben vom Rektor

NR_52 **JAHRGANG 51**
27. Juni 2022

Leitlinie zur Informationssicherheit

vom 27.06.2022

Auf Grund des § 2 Abs. 4 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) vom 16.09.2014 (GV. NRW. S. 547), zuletzt geändert am 25.11.2021 (GV. NRW. S. 1210a), hat die Bergische Universität Wuppertal die folgende Leitlinie erlassen.

Inhaltsübersicht

1. Präambel und Geltungsbereich

Die Bergische Universität Wuppertal ist eine moderne, aufstrebende Forschungsuniversität mit internationalen Ambitionen und gleichzeitig anhaltendem Bekenntnis zu einer humboldtschen Bildungstradition zeitgemäßer Auslegung. Ihre wachsende Forschungsstärke sowie ihr hoher Qualitätsanspruch an Studium und Lehre spielen für die Bergische Universität ebenso eine bedeutende Rolle wie der nachhaltige Wissens- und Technologietransfer als Teil des gesellschaftlichen Auftrags und im Bewusstsein regionaler Verantwortung.

Im Zuge der COVID-19-Pandemie seit März 2020 ist die Bedeutung von digitalen Lösungen zur Erfüllung des universitären Auftrags deutlich gestiegen. Digitale Instrumente und Formate unterstützen dabei nicht nur die Lehre, die Forschung und den Transfer, sondern auch das Management und die Verwaltung der Bergischen Universität, wie in der Digitalisierungsstrategie niedergelegt.

Die vorliegende Leitlinie zur Informationssicherheit richtet sich an alle Mitglieder und Angehörigen der Bergischen Universität. Sie wurde durch das Rektorat beschlossen, das die Maßnahmen zur Erhöhung der Informationssicherheit unterstützt und damit zu einem sicheren Umgang mit Informationen sowie zu einer sicheren Nutzung digitaler Lösungen und zum sicheren IT-Betrieb an der Bergischen Universität beiträgt.

2. Stellenwert der Informationssicherheit an der Bergischen Universität

Informationssicherheit ist für die Bergische Universität von entscheidender Bedeutung, weil alle wesentlichen strategischen und operativen Geschäftsprozesse an der modernen Universität durch Informationstechnologie (IT) maßgeblich unterstützt werden.

Zudem will die Bergische Universität zum einen die in den letzten zwei Jahren erarbeiteten Digitalisierungsbestrebungen im Dienst einer bestmöglichen Erreichung ihrer strategischen Ziele kontinuierlich weiterentwickeln. Zum anderen erfordern auch gesetzliche Rahmenbedingungen wie beispielsweise das E-Government-Gesetz Nordrhein-Westfalen (EGovG NRW) und das Onlinezugangsgesetz (OZG) die (weitere) Digitalisierung der universitären Verwaltungsprozesse.

Bei allen Chancen, welche die Nutzung digitaler Werkzeuge und Formate für die Bergische Universität mit sich bringt, dürfen die anwachsenden Risiken durch eine zunehmende Abhängigkeit der Prozesse von funktionierenden IT-Lösungen nicht außer Acht gelassen werden. Aus dem umfangreichen Einsatz digitaler Lösungen erwächst ein hoher Anspruch an die Verfügbarkeit, die Vertraulichkeit und die Integrität der verarbeiteten Informationen, IT-Prozesse und IT-Systeme an der Bergischen Universität. Nicht zuletzt sind sichere IT-Prozesse eine Grundvoraussetzung für alle technischen und organisatorischen Datenschutzmaßnahmen, die bei der Verarbeitung personenbezogener Daten umzusetzen sind.

Die vorliegende Leitlinie zur Informationssicherheit dient diesem Anspruch und wahrt dabei die positiv-kooperative und Vielfalt schätzende Organisationskultur. Einschränkungen der Nutzung und des Betriebs von IT-Anwendungen, IT-Systemen und Dienstleistungen erfolgen nur soweit, wie es zur Erreichung der Schutzziele der Informationssicherheit und der strategischen Ziele der Bergischen Universität unbedingt erforderlich ist.

3. Schutzziele

Durch die Fülle an unterschiedlichen IT-Systemen, Anwendungen, Nutzer*innen sowie zu verarbeitenden Informationen an der Bergischen Universität stellt diese ein sehr interessantes und vielfältiges Ziel für Cyberangriffe von innen und außen dar. Neben der Defensive solcher Informationssicherheitsangriffe ist die Aufrechterhaltung des Universitätsbetriebs im Rahmen von Forschung, Lehre, Transfer, Management und Verwaltung ein substanzielles Ziel der Informationssicherheit.

Ziel der Bergischen Universität ist die Gewährleistung von verfügbaren Daten und IT-Systemen in allen relevanten Bereichen, sodass potentielle Ausfallzeiten und Datenverlust auf ein tolerierbares Maß beschränkt werden. Darüber hinaus ist es äußerst wichtig, die Integrität und Vertraulichkeit von sensiblen Universitätsdaten und personenbezogenen Daten in ausreichender Weise zu garantieren.

Hierzu gehören Personal- und Studierendendaten ebenso wie technische Unterlagen oder Forschungsdaten.
Schadensfälle mit hohen finanziellen Auswirkungen und immaterielle Folgen wie beispielsweise Imageschäden für die Bergische Universität müssen verhindert werden. Die Verfügbarkeit, Vertraulichkeit und Integrität werden dabei nicht nur durch externe Angreifende bedroht, sondern können auch durch interne Schwachstellen gefährdet werden. Durch die Umsetzung von geeigneten Sicherheitsmaßnahmen soll dem jeweiligen Schutzziel angemessene und dem Stand der Technik entsprechende Informationssicherheit gewährleistet werden.

Zusammenfassend werden mit dieser Leitlinie zur Informationssicherheit die folgenden Schutzziele verfolgt:

- **Verfügbarkeit:**
  Informationen, IT-Systeme und Anwendungen stehen den berechtigten Nutzer*innen zur Verfügung, sind bei Bedarf zugänglich und nutzbar. Systemausfälle werden vermieden.
- **Vertraulichkeit:**
  Informationen dürfen lediglich von autorisierten Nutzer*innen gelesen bzw. verändert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten als auch während der Datenübertragung. Informationen sind nicht von Dritten einsehbar und vor unberechtigter Offenlegung geschützt.
- **Integrität:**
  Informationen dürfen nicht unbemerkt verändert werden.
- **Datenschutz:**
  Personenbezogene Daten werden bei der Speicherung, dem Transfer, der Korrektur sowie Löschung vor Missbrauch geschützt.

4. Informationssicherheitsstrategie

Die Informationssicherheitsstrategie der Bergischen Universität stützt sich wie alle anderen Teilstrategien auf das im Leitbild formulierte Selbstverständnis und die damit verbundenen Werthaltungen. Sie besteht im Wesentlichen darin, sich mit wirtschaftlichem Ressourceneinsatz einem möglichst hohen Maß an Informationssicherheit zu nähern und verbleibende Restrisiken auf ein akzeptables Maß zu minimieren. Bei der Erreichung der oben genannten Schutzziele ist die Verhältnismäßigkeit der eingesetzten Maßnahmen zum Wert der zu schützenden Güter zu berücksichtigen.

Kernelement der Informationssicherheitsstrategie ist ein kontinuierlicher Informationssicherheitsprozess. Dieser wird durch die Einführung eines universitätsweiten auf die Organisationskultur der Bergischen Universität angepassten Informationssicherheitsmanagementsystems (ISMS) initiiert. Das ISMS orientiert sich dabei am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Umsetzung erfolgt schrittweise und konzentriert sich zunächst auf die zentrale IT (ZIM) sowie die Verwaltungs-IT (Dezernat 7).

Als Kern der Informationssicherheitsstrategie umfasst das ISMS folgende wesentliche Elemente:

- **Sensibilisierung der Mitglieder und Angehörigen der Bergischen Universität:**
  Die Mitglieder und Angehörigen der Bergischen Universität werden durch Informations- und Beratungsangebote sowie Schulungen befähigt, die Bedeutung von Informationssicherheit im Rahmen ihrer Tätigkeiten nachzuempfinden, die Erfordernis von Sicherheitsmaßnahmen zu verstehen und ihr eigenes Verhalten an den Informationssicherheitszielen der Bergischen Universität auszurichten. Erkennen die Mitglieder Angriffe auf Informationen oder unterlaufen ihnen Fehler im Umgang mit schützenswerten Informationen, informieren sie umgehend die*den Informationssicherheitsbeauftragten.
- **Schutzbedarfsfeststellung:**
  Um sowohl universitätsinternen als auch externen (z. B. vertraglichen) Anforderungen zu entsprechen, wird in einem strukturierten Verfahren festgelegt, welchen Schutzbedarf eine bestimmte Information hat und welchen Bedrohungen sie ausgesetzt ist. Auf dieser Basis werden angemessene Informationssicherheitsmaßnahmen definiert und umgesetzt.

- **Aktuelle Software und IT-Systeme:**
  Die Informationssysteme der Bergischen Universität werden auf einem aktuellen und sicheren Stand gehalten. Eine schnellstmögliche Schließung von bekannt gewordenen Sicherheitslücken erschwert so Angriffe auf die schützenswerten Informationen der Bergischen Universität.

- **Vorfallmanagement:**
  Für die Bearbeitung von Informationssicherheitsvorfällen werden Verantwortliche bestimmt und verbindliche Prozesse definiert.

- **Notfallmanagement:**
  Die Wiederaufnahme des Universitätsbetriebs in Not- und Krisenfällen der Informationssicherheit wird durch Notfallkonzepte und -pläne sichergestellt.

- **Regelmäßige Überprüfung der Sicherheitsmaßnahmen:**
  Im Sinne eines kontinuierlichen Verbesserungsprozesses werden, aufgrund der rasanten Veränderung von Bedrohungen im Cyberraum und den damit verbundenen Risiken, aber auch im Rahmen von Umstrukturierungen an der Bergischen Universität sowie die Einführung neuer IT-Systeme und -Anwendungen, die definierten Informationssicherheitsmaßnahmen regelmäßig auf ihre Wirksamkeit hin überprüft und bei Bedarf angepasst.

Im Zuge des Informationssicherheitsmanagementsystems an der Bergischen Universität werden die Regelungen zur Informationssicherheit in unterschiedlichen Dokumenten aggregiert:

- Leitlinie zur Informationssicherheit,
- Informationssicherheitskonzept sowie
- Richtlinien zur Informationssicherheit.

Die Informationssicherheitsleitlinie (dieses Dokument) beschreibt allgemein die strategischen Informationssicherheitsziele der Bergischen Universität und die Verantwortlichkeiten zur universitätsweiten Sicherstellung von Informationssicherheit.

Das Informationssicherheitskonzept konkretisiert als zentrales Dokument des ISMS die Sicherheitsverantwortlichen sowie -prozesse und veranschaulicht verbindliche, technische, personelle und organisatorische Maßnahmen zur universitätsübergreifenden Gewährleistung von Informationssicherheit.

Die Richtlinien zur Informationssicherheit definieren technische, personelle und organisatorische Maßnahmen in Bezug auf einzelne Geschäftsprozesse, IT-Services, Systeme oder Anwendungen.

5. Verantwortlichkeiten

5.1 Rektorat

Als Universitätsleitung trägt das Rektorat die Gesamtverantwortung für die Informationssicherheit an der Bergischen Universität. Es erlässt verbindliche Regeln zur Informationssicherheit für die Bergische Universität und macht diese amtlich bei den Mitgliedern und Angehörigen bekannt. Das Rektorat gewährleistet jederzeit die Option zur Kenntnisnahme der aktuellen Vorgaben, indem diese in den amtlichen Mitteilungen der Bergischen Universität veröffentlicht werden. Darüber hinaus trägt die Universitätsleitung Sorge dafür, dass sich unter den Mitgliedern und Angehörigen der Bergischen Universität eine „Kultur der Informationssicherheit“ entwickelt.

Aus dem Kreis der Prorektor*innen wird ein*e Ansprechpartner*in für Informationssicherheit benannt, welche*r die Anliegen der Informationssicherheit auf professoraler Ebene vertritt.

5.2 Informationssicherheitsbeauftragte*r

Die*der Informationssicherheitsbeauftragte übernimmt als Stabsstelle des Rektorats eine steuernde Funktion und koordiniert die universitätsweiten Informationssicherheitsprozesse. Sie*er unterstützt in Zusammenarbeit mit der Referentin für Informationssicherheit das Rektorat, die Fakultäten und die Einrichtungen der Bergischen Universität bei deren Aufgaben bezüglich der

Informationssicherheit. Hierfür besitzt die*der Informationssicherheitsbeauftragte ein breites fachliches Wissen, kennt sich mit einschlägigen rechtlichen und technischen Rahmenbedingungen aus, und ist mit dem Universitätsbetrieb vertraut.

Sie*er initiiert die Verabschiedung von Richtlinien sowie Regelungen zur Informationssicherheit durch das Rektorat und begleitet die Realisierung entsprechender Informationssicherheitsmaßnahmen. Die*der Informationssicherheitsbeauftragte trägt die Verantwortung für die Reaktion auf sowie die Untersuchung von Sicherheitsvorfällen. Sie*er berichtet regelmäßig im CIO-Team über ihre*seine Aktivitäten. Bei der Erstellung von Rektoratsvorlagen beteiligt sie*er das CIO-Team, welches Stellungnahmen und Empfehlungen zur praktischen Umsetzbarkeit abgeben kann. Die*der ISB berichtet regelmäßig an das Rektorat über den Status quo der Informationssicherheit an der Bergischen Universität.

Die*der Informationssicherheitsbeauftragte

- ist in allen für die Informationssicherheit relevanten Themen zu informieren,
- ist bei grundlegenden Entscheidungen, Vorhaben und Änderungen, die die Informationssicherheit berühren können (z. B. neue IT- Projekte, Änderungen der IT-Infrastruktur, Änderungen von Rahmenbedingungen mit Auswirkungen auf die Informationssicherheit, …), frühzeitig einzubeziehen und anzuhören. Ihre*seine Empfehlungen sind bei den Entscheidungen nach Möglichkeit umzusetzen. Sollte die zuständige Organisationseinheit von den Empfehlungen der*des ISB abweichen wollen, ist dies vorab mit der*dem ISB abzustimmen und zu dokumentieren. Bei Divergenzen, die nicht zwischen der*dem ISB und der zuständigen Organisationseinheit geklärt werden können, vermittelt zunächst die Ansprechperson für Informationssicherheit aus dem Kreis der Prorektor*innen. Im Konfliktfall entscheidet das Rektorat,
- ist Mitglied im Risikoausschuss der Bergischen Universität.

5.3 Referent*in Informationssicherheit

Die*der Referent*in für Informationssicherheit, angesiedelt in der Stabsstelle des Rektorats „UniService Digitale Transformation“, unterstützt die*den Informationssicherheitsbeauftragten konzeptionell. Sie*er entwickelt entsprechende Konzepte, Strategien und Maßnahmen, welche die Bergische Universität bei der Erreichung ihrer Ziele gesetzeskonform und unter Aufrechterhaltung ihrer Informationssicherheits-standards stärken. Die*der Referent*in für Informationssicherheit berät, unterstützt und schult die Einrichtungen sowie Mitarbeiter*innen in Fragen der Informationssicherheit durch Gesprächs- und Schulungsangebote, die Erstellung von Handreichungen, Leitfäden sowie Expertisen.

5.4 Mitarbeiter*in für IT-Sicherheit

Die*der Mitarbeiter*in für IT-Sicherheit bildet im ZIM die Schnittstelle zur*m Informationssicherheitsbeauftragten sowie der*dem Referent*in für Informationssicherheit. Sie*er überwacht die IT-Sicherheit der sowie mögliche Bedrohungen für die Bergische Universität und entwickelt das Sicherheitsniveau stetig weiter. Die*der Mitarbeiter*in für IT-Sicherheit begleitet abteilungsübergreifende Change-Projekte zur IT-Sicherheit der gesamten Universität und erstellt Empfehlungen zur Erhöhung der IT-Sicherheit, auch für die Fakultäten der Bergischen Universität. Sie*er setzt vorbeugende Maßnahmen gegen Sicherheitsvorfälle und Notfälle um, darunter auch einen Notfallwiederherstellungsplan, und unterstützt von technischer Seite die*den Informationssicherheitsbeauftragten bei der Bearbeitung von Sicherheitsvorfällen.

5.5 Leitungen des Zentrums für Informations- und Medienverarbeitung, der Universitätsbibliothek sowie der Verwaltungs-IT (Dezernat 7)

Eine zentrale Bedeutung für die operative IT-Sicherheit hat die Leitung des Zentrums für Informations- und Medienverarbeitung (ZIM). Sie ist für den sicheren Betrieb der zentralen IT und die Umsetzung geeigneter technischer Sicherheitsmaßnahmen verantwortlich. Für die Verwaltungs-IT übernimmt die Leitung des Dezernats 7 (Organisationsentwicklung und Informationstechnik) sowie für die IT-Systeme der Universitätsbibliothek übernimmt die Bibliotheksleitung

die Verantwortung für einen sicheren IT-Betrieb. Alle Leitungen stellen sicher, dass die*der Informationssicherheitsbeauftragte frühzeitig in die zentralen IT-Projekte eingebunden wird.

5.6 Personen mit Führungsverantwortung

Personen mit Führungsverantwortung sind verantwortlich für die Umsetzung von Informationssicherheit in ihrem Bereich und gehen mit gutem Beispiel voran. Führungskräfte, in deren Bereich IT-Infrastruktur eigenverantwortlich betrieben wird, verantworten den sicheren Betrieb dieser IT und setzen geeignete technische Sicherheitsmaßnahmen um.

5.7 Koordinator*innen für Informationssicherheit

In den Fakultäten und Einrichtungen können durch die jeweiligen Organisationseinheiten Koordinator*innen für Informationssicherheit ernannt werden. Diese unterstützen bei der Umsetzung der vereinbarten Maßnahmen zur Sicherstellung von Informationssicherheit in ihren Bereichen und geben der*dem Informationssicherheitsbeauftragten Rückmeldungen zur praktischen Umsetzbarkeit sowie eventuell notwendigen Anpassungen an den Maßnahmen.

5.8 Mitglieder und Angehörige der Bergischen Universität

Die Mitglieder und Angehörigen der Bergischen Universität entwickeln u.a. durch das Vorbild der Universitätsleitung eine „Kultur der Informationssicherheit“ und nehmen die Informations- und Schulungsangebote zur Informationssicherheit wahr. Sie verhalten sich jederzeit so, dass Informationssicherheit in ihrem Aufgaben- und Verantwortungsbereich sichergestellt ist. Die Einhaltung interner Vorgaben aus dieser Leitlinie und weitergehender Richtlinien sowie Gesetze zur Informationssicherheit ist für sie ein selbstverständlicher Teil ihrer Arbeit. Informationssicherheitsrelevante Vorfälle oder potenzielle Sicherheitsrisiken melden sie unverzüglich auf dem Dienstweg.

6. Aktualisierung der Informationssicherheitsleitlinie

Die Leitlinie zur Informationssicherheit wird regelmäßig, spätestens alle zwei Jahre, auf ihre Aktualität hin überprüft und bei Bedarf angepasst. Überarbeitungen sind beispielsweise bei wesentlichen Veränderungen der universitären Strukturen oder Prozesse notwendig.

7. In-Kraft-Treten

Diese Leitlinie zur Informationssicherheit tritt am Tag nach ihrer Veröffentlichung in den Amtlichen Mitteilungen als Verkündungsblatt der Bergischen Universität Wuppertal in Kraft.

Ausgefertigt auf Grund des Beschlusses des Rektorates der Bergischen Universität Wuppertal vom 22.06.2022.

Wuppertal, den 27.06.2022

Der Rektor
der Bergischen Universität Wuppertal
Universitätsprofessor Dr. Dr. h.c. Lambert T. Koch