

Informationssicherheitsleitlinie der Universität Mannheim

Ausfertigungsdatum:

Mai 2025

Stand:

Bislang keine Änderungen

Fundstellen:

Original vom Mai 2025: Bekanntmachungen des Rektorats (BekR) Nr. 05/2025, Seite 37ff.

Bei der vorliegenden Version handelt es sich um eine nichtamtliche Lesefassung, in der die oben genannten Änderungssatzungen eingearbeitet sind. Maßgeblich und rechtlich verbindlich ist weiterhin nur der in den Bekanntmachungen des Rektorats veröffentlichte Text.

Inhalt

1 Präambel	2
2 Geltungsbereich	2
3 Ziel der Informationssicherheit	2
4 Vorgehen im Informationssicherheitsprozess	3
5 Einordnung dieser Informationssicherheitsleitlinie	3
5.1 Informationssicherheitsleitlinie	4
5.2 Informationssicherheitsstrategie	4
5.3 Informationssicherheitsrichtlinien	4
6 Rollen und Verantwortlichkeiten	4
6.1 Allgemeingültige Verantwortlichkeiten	5
6.2 Chief Information Security Officer	5
6.3 Rektorat	6
6.4 Lenkungsausschuss für Informationssicherheit	7
6.5 Universitäts-IT	7
7 Kooperationen	7

1 Präambel

¹Die Universität Mannheim bildet seit Generationen Fachkräfte für Wirtschaft, Wissenschaft und Gesellschaft aus und zählt zu den besten Forschungseinrichtungen in Europa. ²Das Gut „Information“ spielt dabei für Forschung, Lehre und Verwaltung eine zentrale Rolle. ³Information umfasst sowohl die Kenntnisse der Beschäftigten als auch papiergebundenes und durch Informationstechnologie (IT) verarbeitetes Wissen. ⁴Durch einen stetig moderner gestalteten Universitätsbetrieb hat sich eine hohe Abhängigkeit von einer funktionierenden und sicheren IT entwickelt. ⁵Diese Abhängigkeit wird Tag für Tag durch unterschiedlichste Schwachstellen und Bedrohungen¹ auf die Probe gestellt. ⁶Insbesondere versuchen Angreifende, den Universitätsbetrieb durch Cyberangriffe zum Stillstand zu bringen. ⁷Informationssicherheit dient dabei der Gewährleistung eines sicheren und störungsarmen Betriebs. ⁸Mit dieser Informationssicherheitsleitlinie bekundet das Rektorat der Universität Mannheim den hohen Stellenwert der Informationssicherheit und des dazugehörigen Informationssicherheitsmanagements für die Universität. ⁹Damit legt diese Leitlinie den Grundstein für das Informationssicherheitsmanagement an der Universität Mannheim.

2 Geltungsbereich

¹Diese Leitlinie sowie die auf der Leitlinie beruhenden Richtlinien gelten für die gesamte Universität Mannheim. ²Sie gilt für alle Personen, auch Dritte, die Informationen der Universität verarbeiten bzw. deren informationsverarbeitende Systeme oder Prozesse nutzen. ³Für Beschäftigte gilt die Informationssicherheitsleitlinie durch die Veröffentlichung und muss unverzüglich eingehalten werden. ⁴Ab Inkrafttreten der Informationssicherheitsleitlinie sollen Dritte, soweit sie als Auftragnehmer für die Universität Leistungen erbringen, bei neu erfolgenden Ausschreibungen und Auftragserteilungen auf die Vorgaben dieser Informationssicherheitsleitlinie im notwendigen und sinnvollem Umfang verpflichtet werden.

3 Ziel der Informationssicherheit

¹Die Handlungsfähigkeit der Universität, also den Forschungs-, Lehr- und Verwaltungsbetrieb so unterbrechungsfrei wie möglich aufrechtzuerhalten, ist ein zentrales Ziel der

¹ Dies sind zum Beispiel: Physische Bedrohungen, menschliche Fehler, technische Fehler und Ausfälle, Social Engineering, Schadsoftware, unzureichende Sicherheitsrichtlinien oder veraltete Software.

Informationssicherheit. ²Dabei steht im Vordergrund, die drei Schutzziele Vertraulichkeit², Integrität³ und Verfügbarkeit⁴ in einem angemessenen Rahmen sicherzustellen, auch wenn absolute Sicherheit nicht vollständig gewährleistet werden kann. ³Eine Verletzung jedes dieser Schutzziele, zum Beispiel in Form einer Offenlegung vertraulicher Informationen, einer Manipulation von Systemen bzw. Informationen oder eines Verlusts von Daten, verursacht eine Störung des regulären Universitätsbetriebs.

4 Vorgehen im Informationssicherheitsprozess

¹Informationssicherheit ist kein erreichbarer Zustand. ²Für ihre weitgehende Sicherstellung muss sie im Rahmen eines kontinuierlich ablaufenden Prozesses stetig gepflegt und weiterentwickelt werden. ³Die Universität Mannheim verfolgt dabei einen risikobasierten Ansatz. ⁴Im Fokus des Prozesses steht die Handlungsfähigkeit der Universität. ⁵Von ihr leiten sich die strategischen Ziele der Informationssicherheit ab und werden in der Informationssicherheitsstrategie der Universität Mannheim festgeschrieben. ⁶Zu den strategischen Zielen werden risikobasiert Maßnahmen zum Schutz der Universität entwickelt. ⁷Sie bilden die Ausgangslage für das weitere Vorgehen. ⁸Diese Maßnahmen werden anschließend so priorisiert, dass unter Berücksichtigung der zur Verfügung stehenden Ressourcen ein maximaler Sicherheitsgewinn erzielt werden kann. ⁹Priorisierung und Maßnahmen werden regelmäßig auf ihre Wirksamkeit überprüft und bei Bedarf angepasst.

5 Einordnung dieser Informationssicherheitsleitlinie

¹In den folgenden Absätzen werden Informationssicherheitsleitlinie, Informationssicherheitsstrategie und Informationssicherheitsrichtlinien beschrieben und voneinander abgegrenzt. ²Dabei befinden sich die Informationssicherheitsleitlinie und die Informationssicherheitsstrategie auf der gleichen Geltungsebene. ³Die Informationssicherheitsrichtlinien sind der Leitlinie untergeordnet.

² „Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein“ (Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, 2. Edition 2023)

³ „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. [...] Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zur verfassenden Person verfälscht oder Zeitangaben zur Erstellung manipuliert wurden“ (Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, 2. Edition 2023)

⁴ „Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendenden stets wie vorgesehen genutzt werden können“ (Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, 2. Edition 2023)

5.1 Informationssicherheitsleitlinie

¹Mit dem Bekenntnis des Rektorats zur Informationssicherheit bildet diese Leitlinie die Grundlage für alle weiteren Strukturen, Abläufe, Maßnahmen und Richtlinien der Informationssicherheit. ²Dazu beschreibt sie die Akteure der Informationssicherheit und deren Verantwortlichkeiten sowie das gewählte Vorgehen zur Realisierung der Informationssicherheit an der Universität Mannheim.

5.2 Informationssicherheitsstrategie

¹Eine Konkretisierung des zentralen Informationssicherheitsziels findet in der jeweils aktuell gültigen Informationssicherheitsstrategie der Universität Mannheim statt. ²Sie definiert die strategischen Ziele der Universität mit Blick auf die Informationssicherheit und dazugehörige Maßnahmen zu deren Realisierung. ³Damit sichergestellt ist, dass sowohl der aktuelle Stand der Technik als auch aktuelle Risiken und Angriffsszenarien bei der Auswahl umzusetzender Maßnahmen berücksichtigt werden, wird die Informationssicherheitsstrategie grundsätzlich alle vier Jahre überarbeitet.

5.3 Informationssicherheitsrichtlinien

¹Informationssicherheitsrichtlinien beschreiben konkrete Vorgaben und Handlungsanweisungen zu einem bestimmten Thema und für eine definierte Zielgruppe. ²Sie sind essenziell, um Maßnahmen über die gesamte Universität hinweg sicherzustellen und somit die Handlungsfähigkeit der Universität zu erhalten.

6 Rollen und Verantwortlichkeiten

¹Neben allgemeingültigen Verantwortlichkeiten, die jede Person im Geltungsbereich betreffen, gibt es spezielle Rollen mit besonderen Verantwortlichkeiten. ²Dieses Kapitel beschreibt zunächst die allgemeingültigen Verantwortlichkeiten und im Anschluss die speziellen Rollen. ³Das Rektorat trägt die Gesamtverantwortung für Informationssicherheit und hat mit dem Lenkungsausschuss für Informationssicherheit ein Gremium geschaffen, das die Informationssicherheit auf strategischer Ebene steuert. ⁴Weiterhin gibt es an der Universität Mannheim eine gesonderte Stabsstelle Informationssicherheit mit der*dem Chief Information Security Officer (CISO⁵) als Leitung. ⁵Die Universitäts-IT trägt mit ihrer Rolle als zentrale IT-Dienstleisterin eine besondere Verantwortung bei der Absicherung der universitären IT, insbesondere der zentralen IT-Infrastruktur.

⁵ Chief Information Security Officer, in der Regel verwendetes englisches Akronym für die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten.

6.1 Allgemeingültige Verantwortlichkeiten

¹Der effektive Schutz von Informationen bedarf der Mitwirkung aller. ²Jede Person, die in den Geltungsbereich dieser Leitlinie fällt, muss im Rahmen ihrer Entscheidungsbefugnisse nach bestem Wissen für die Berücksichtigung und den Erhalt der Informationssicherheit sowie die Umsetzung notwendiger Sicherheitsmaßnahmen Sorge tragen. ³Dies verpflichtet insbesondere auch die Universitäts-IT und alle weiteren Betreiber*innen von IT-Systemen und deren Infrastruktur, technische und organisatorische Maßnahmen zu deren Schutz zu realisieren. ⁴Bei Bedarf unterstützt die*der Chief Information Security Officer die technische Realisierung auf organisatorischer Ebene bzw. berät das zuständige Personal. ⁵Ergänzend wird, wenn nötig, Kontakt zu Dienstleistern hergestellt oder auf Schulungsmaterial verwiesen. ⁶Damit die Universität den Umsetzungsstand von Maßnahmen zur Erhöhung der Informationssicherheit nachvollziehen und steuern kann, sind Dokumentationen dieser Maßnahmen von den jeweiligen verantwortlichen Personen und Einrichtungen in dafür geeigneter Form zu erstellen und aktuell zu halten. ⁷Bei Schwachstellen⁶ und negativen, sicherheitsrelevanten Ereignissen⁷, die potenziell die Sicherheit der Universität, ihrer Angehörigen, ihrer Systeme oder ihrer Daten, gefährden, ist die frühzeitige Einbindung der*des CISO von hoher Wichtigkeit, um eine adäquate Reaktion zu gewährleisten. ⁸Sie sind daher unverzüglich bei der*dem CISO zu melden. ⁹Bei der Konzeption von Projekten und Dauertätigkeiten sind Zeit und Budget für das Thema Informationssicherheit adäquat zu berücksichtigen. ¹⁰Bei Bedarf kann die*der CISO die individuelle Planung unterstützen, um eine ausreichende Beachtung sicherzustellen.

6.2 Chief Information Security Officer

¹Die*der Chief Information Security Officer (CISO), oft auch Informationssicherheitsbeauftragte*r genannt, leitet die Stabsstelle Informationssicherheit. ²Sie*Er steuert die Umsetzung der Informationssicherheit an der Universität Mannheim innerhalb des Rahmens, der durch diese Leitlinie, die Strategie für Informationssicherheit und die strategischen Entscheidungen des Lenkungsausschusses für Informationssicherheit vorgegeben wird, und ist beratend tätig. ³Um Informationssicherheit nachhaltig an der Universität zu etablieren, werden organisatorische und technische Maßnahmen und Prozesse zur Sicherstellung der Informationssicherheit durch die*den CISO strategisch geplant und überwacht. ⁴Die konkrete Planung, Umsetzung und kontinuierliche Verbesserung fällt je nach Maßnahme und Prozess in den Aufgabenbereich der*des CISOs, der UNIT oder weiterer Einrichtungen bzw. Personen. ⁵Im Verantwortungsbereich der*des CISO liegen dabei insbesondere die organisatorischen Aspekte der Informationssicherheit. ⁶Darunter fallen

⁶ Eine Schwäche oder ein Fehler in einer Anwendung, einem IT-System, einer Komponente, einer Netzwerkinfrastruktur oder einem Prozess, die von Angreifenden ausgenutzt werden können.

⁷ Beispiele für zu meldende negative Ereignisse sind: gestohlener Laptop, Computer mit Trojanerbefall, kompromittierte Server, Reaktionen auf Phishing-Mails und generell abgeflossene Daten.

unter anderem das Steuern des Informationssicherheitsprozesses, Beratungsaufgaben, die Planung und Umsetzung von Awareness- und Schulungsmaßnahmen sowie die Abwicklung von Informationssicherheitsvorfällen. ⁷Außerdem erstellt und aktualisiert die*der CISO die Informationssicherheitsleitlinie und die Informationssicherheitsstrategie, die anschließend dem Rektorat als Entwurf zur Verabschiedung vorgelegt werden. ⁸Die Erstellung der universitätsweiten Informationssicherheitsrichtlinien wird durch sie*ihn koordiniert und unterstützt. ⁹Die konkrete Erstellung einer Richtlinie findet in Abstimmung mit der*dem CISO durch die jeweiligen verantwortlichen Personen und Einrichtungen statt. ¹⁰Die erstellten Dokumente werden durch die*den CISO in Abstimmung mit dem Lenkungsausschuss für Informationssicherheit dem Rektorat zur Verabschiedung und Freigabe vorgelegt. ¹¹Mindestens einmal jährlich berichtet die*der CISO den aktuellen Stand der Informationssicherheit an der Universität direkt an das Rektorat. ¹²Mögliche Interessenskonflikte müssen bei der Auswahl der*des CISO vermieden werden. ¹³Insbesondere darf die*der CISO keine weiteren Rollen wahrnehmen, die zu solchen Konflikten führen können. ¹⁴Dies schließt unter anderem die Rolle der*des Chief Information Officer (CIO) sowie der Leitung der Universitäts-IT aus. ¹⁵Damit die*der CISO ihre*seine Funktion adäquat wahrnehmen kann, muss sie*er unabhängig sein. ¹⁶Das bedeutet, dass Vorgesetzte keinen Einfluss auf Gutachten oder Bewertungen der Informationssicherheit nehmen dürfen. ¹⁷Zur Gewährleistung dieser Unabhängigkeit sind fachliche, disziplinarische und finanzielle Aspekte zu berücksichtigen.

6.3 Rektorat

¹Das Rektorat trägt die Verantwortung für die Informationssicherheit an der Universität Mannheim. ²Es stellt sicher, dass Informationssicherheit, entsprechend dieser Leitlinie, an der Universität Mannheim realisiert, erhalten und weiterentwickelt wird. ³Das Rektorat empfängt die Berichte der*des CISO. ⁴Der darin beschriebene Stand der Informationssicherheit an der Universität Mannheim wird mindestens einmal jährlich durch das Rektorat geprüft, um sicherzustellen, dass es seiner in dieser Leitlinie beschriebenen Verantwortung adäquat nachkommt. ⁵Die Informationssicherheitsleitlinie und die Informationssicherheitsstrategie werden durch das Rektorat verabschiedet und freigegeben. ⁶Auch universitätsweite Informationssicherheitsrichtlinien werden durch das Rektorat freigegeben. ⁷Die Befugnis zur Freigabe einer Richtlinie kann an andere Stellen oder Rollen delegiert werden. ⁸Das Rektorat ist dafür verantwortlich, dass die Ressourcen für die Umsetzung und den Erhalt der Informationssicherheit verfügbar sind. ⁹Der*dem CISO und der Universitäts- IT werden durch das Rektorat, nach Abwägung des gesamten Aufgabenspektrums der Universität, finanzielle und zeitliche Ressourcen zur Verfügung gestellt, damit sie regelmäßige Weiterbildungen und Informationsbeschaffungen sowie die Realisierung der in der Informationssicherheitsstrategie der Universität Mannheim beschriebenen Ziele und Maßnahmen im wirtschaftlich sinnvollen Umfang wahrnehmen können.

6.4 Lenkungsausschuss für Informationssicherheit

¹Aufgabe des Lenkungsausschusses ist es, die Maßnahmen der Informationssicherheitsstrategie sowie neue, bisher nicht in der Strategie berücksichtigte Maßnahmen zu priorisieren, deren Status zu prüfen und, wenn nötig, Entscheidungsvorschläge für das Rektorat zu erarbeiten. ²Die Ausarbeitung der einzelnen Vorlagen für das Rektorat obliegt den für die jeweilige Maßnahme verantwortlichen Einrichtungen bzw. Personen. ³Die Mitglieder des Lenkungsausschusses für Informationssicherheit sind kraft Amtes:

- CISO (Geschäftsführung),
- Kanzler*in,
- für Informationssicherheit zuständiges Prorektorat,
- CIO,
- Leitung der Universitäts-IT begleitet von der zuständigen Person für operative IT-Sicherheit.

6.5 Universitäts-IT

¹Die Universitäts-IT ist verantwortlich für die zentrale IT-Infrastruktur der Universität. ²Ihre Aufgabe ist es, die nötigen technischen Strukturen und Abläufe zum Schutz der Informationssicherheit zu schaffen und die dazu nötigen technischen Maßnahmen umzusetzen. ³Dazu steht die Universitäts-IT in engem Kontakt mit der*dem CISO.

7 Kooperationen

¹Da alle Hochschulen im Land bei der Etablierung der Informationssicherheit vor ähnlichen Herausforderungen stehen, soll durch die*den CISO ein regelmäßiger Austausch mit den relevanten Akteuren auf Landesebene stattfinden. ²So können, trotz lokaler Unterschiede der Hochschulen, Synergien genutzt werden. ³Dies soll durch bwInfoSec, den Kooperationsverbund für Informationssicherheit der Universitäten und Hochschulen in Baden-Württemberg, zusätzlich unterstützt werden. ⁴Die*der CISO soll im Rahmen des Kooperationsverbundes an der gezielten Zusammenarbeit zwischen den CISOs und den lokalen Beschäftigten für Informationssicherheit teilnehmen und gemeinsam passende Lösungen erarbeiten. ⁵Auch über den Kooperationsverbund und die Landesgrenzen hinaus soll die*der CISO sich kontinuierlich mit anderen Hochschulen und Universitäten austauschen.

8 Inkrafttreten

[nicht wiedergegeben]