UNIVERSITÄT MANNHEIM

Informationssicherheitsleitlinie

der Universität Mannheim

Foto: Norbert Bach

Version 1.0 vom 02.04.2025
Dokumentenklassifizierung: TLP white – öffentlich

Ansprechperson: Stabsstelle Informationssicherheit
E-Mail: infosicherheit@uni-mannheim.de

Dokumentenklassifizierung mit TLP

Dieses Dokument ist mit dem Traffic Light Protocol (TLP) als „TLP white – öffentlich“ klassifiziert. Diese Angabe ist auch auf dem Deckblatt zu finden und ist dort nach der u.a. Tabelle farblich hervorgehoben.

TLP ermöglicht den Autorinnen und Autoren eines Dokumentes, die Bedingungen für dessen Weitergabe zu regeln und so die Sicherheit zu erhöhen. Als Empfängerin oder Empfänger dieses Dokumentes müssen Sie die auf dem Deckblatt getroffene Klassifizierung einhalten. Eine genaue Erklärung der Weitergaberegelungen finden Sie in der folgenden Tabelle.

TLP-Klassifizierung	Weitergaberegelung
TLP white – öffentlich	Dieses Dokument enthält keine vertraulichen Informationen und kann von urheberrechtlichen Aspekten abgesehen ohne Einschränkung weitergegeben und öffentlich zugänglich gemacht werden.
TLP green – intern	Dieses Dokument enthält Informationen, die für den dienstlichen Gebrauch notwendig sind. Es darf an Partner der Universität weitergeben, jedoch nicht veröffentlicht werden.
TLP amber – vertraulich (…)	Dieses Dokument enthält vertrauliche Informationen und darf daher nur einem begrenzten und zuvor definierten Personenkreis (z.B. UNIT, UB, Lehrstuhl X) weitergegeben werden. Eine Weitergabe an Dritte ist nur möglich, wenn der Dritte das Dokument zur Arbeitserfüllung benötigt und ihm diese TLP-Klassifizierung bekannt ist. Der definierte Personenkreis wird bei der Klassifizierung in Klammer ergänzt.
TLP red – streng vertraulich (…)	Dieses Dokument enthält streng vertrauliche Informationen, die nur einem begrenzten und zuvor definierten Personenkreis, meist auch Teilnehmerkreis einer Besprechung, Konferenz oder schriftlichen Korrespondenz (z.B. Rektorat) bereitgestellt werden darf. Eine Weitergabe ist untersagt. Der definierte Personenkreis wird bei der Klassifizierung in Klammer ergänzt.

Inhaltsverzeichnis

1 Präambel

Die Universität Mannheim bildet seit Generationen Fachkräfte für Wirtschaft, Wissenschaft und Gesellschaft aus und zählt zu den besten Forschungseinrichtungen in Europa. Das Gut „Information“ spielt dabei für Forschung, Lehre und Verwaltung eine zentrale Rolle. Information umfasst sowohl die Kenntnisse der Beschäftigten als auch papiergebundenes und durch Informationstechnologie (IT) verarbeitetes Wissen.

Durch einen stetig moderner gestalteten Universitätsbetrieb hat sich eine hohe Abhängigkeit von einer funktionierenden und sicheren IT entwickelt. Diese Abhängigkeit wird Tag für Tag durch unterschiedlichste Schwachstellen und Bedrohungen[1] auf die Probe gestellt. Insbesondere versuchen Angreifende, den Universitätsbetrieb durch Cyberangriffe zum Stillstand zu bringen. Informationssicherheit dient dabei der Gewährleistung eines sicheren und störungsarmen Betriebs.

Mit dieser Informationssicherheitsleitlinie bekundet das Rektorat der Universität Mannheim den hohen Stellenwert der Informationssicherheit und des dazugehörigen Informationssicherheitsmanagements für die Universität.

Damit legt diese Leitlinie den Grundstein für das Informationssicherheitsmanagement an der Universität Mannheim.

2 Geltungsbereich

Diese Leitlinie sowie die auf der Leitlinie beruhenden Richtlinien gelten für die gesamte Universität Mannheim. Sie gilt für alle Personen, auch Dritte, die Informationen der Universität verarbeiten bzw. deren informationsverarbeitende Systeme oder Prozesse nutzen.

Für Beschäftigte gilt die Informationssicherheitsleitlinie durch die Veröffentlichung und muss unverzüglich eingehalten werden.

Ab 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.

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

3 Ziel der Informationssicherheit

Die Handlungsfähigkeit der Universität, also den Forschungs-, Lehr- und Verwaltungsbetrieb so unterbrechungsfrei wie möglich aufrechtzuerhalten, ist ein zentrales Ziel der Informationssicherheit. Dabei steht im Vordergrund, die drei Schutzziele Vertraulichkeit[2], Integrität[3] und Verfügbarkeit[4] in einem angemessenen Rahmen sicherzustellen, auch wenn absolute Sicherheit nicht vollständig gewährleistet werden kann.

Eine 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

Informationssicherheit ist kein erreichbarer Zustand. Für ihre weitgehende Sicherstellung muss sie im Rahmen eines kontinuierlich ablaufenden Prozesses stetig gepflegt und weiterentwickelt werden. Die Universität Mannheim verfolgt dabei einen risikobasierten Ansatz.

Im Fokus des Prozesses steht die Handlungsfähigkeit der Universität. Von ihr leiten sich die strategischen Ziele der Informationssicherheit ab und werden in der Informationssicherheitsstrategie der Universität Mannheim festgeschrieben. Zu den strategischen Zielen werden risikobasiert Maßnahmen zum Schutz der Universität entwickelt. Sie bilden die Ausgangslage für das weitere Vorgehen.

Diese Maßnahmen werden anschließend so priorisiert, dass unter Berücksichtigung der zur Verfügung stehenden Ressourcen ein maximaler Sicherheitsgewinn erzielt werden kann. Priorisierung und Maßnahmen werden regelmäßig auf ihre Wirksamkeit überprüft und bei Bedarf angepasst.

---

[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 Einordnung dieser Informationssicherheitsleitlinie

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

5.1 Informationssicherheitsleitlinie

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

5.2 Informationssicherheitsstrategie

Eine Konkretisierung des zentralen Informationssicherheitsziels findet in der jeweils aktuell gültigen Informationssicherheitsstrategie der Universität Mannheim statt. Sie definiert die strategischen Ziele der Universität mit Blick auf die Informationssicherheit und dazugehörige Maßnahmen zu deren Realisierung. Damit 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

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

6 Rollen und Verantwortlichkeiten

Neben allgemeingültigen Verantwortlichkeiten, die jede Person im Geltungsbereich betreffen, gibt es spezielle Rollen mit besonderen Verantwortlichkeiten. Dieses Kapitel beschreibt zunächst die allgemeingültigen Verantwortlichkeiten und im Anschluss die speziellen Rollen.

Das Rektorat trägt die Gesamtverantwortung für Informationssicherheit und hat mit dem Lenkungsausschuss für Informationssicherheit ein Gremium geschaffen, das die Informationssicherheit auf strategischer Ebene steuert. Weiterhin gibt es an der Universität Mannheim eine gesonderte Stabsstelle Informationssicherheit mit der*dem Chief Information Security Officer (CISO[5]) als Leitung. Die

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

Universitäts-IT trägt mit ihrer Rolle als zentrale IT-Dienstleisterin eine besondere Verantwortung bei der Absicherung der universitären IT, insbesondere der zentralen IT-Infrastruktur.

6.1 Allgemeingültige Verantwortlichkeiten

Der effektive Schutz von Informationen bedarf der Mitwirkung aller. Jede 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. Dies 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. Bei Bedarf unterstützt die*der Chief Information Security Officer die technische Realisierung auf organisatorischer Ebene bzw. berät das zuständige Personal. Ergänzend wird, wenn nötig, Kontakt zu Dienstleistern hergestellt oder auf Schulungsmaterial verwiesen.

Damit 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.

Bei Schwachstellen[6] und negativen, sicherheitsrelevanten Ereignissen[7], 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. Sie sind daher unverzüglich bei der*dem CISO zu melden.

Bei der Konzeption von Projekten und Dauertätigkeiten sind Zeit und Budget für das Thema Informationssicherheit adäquat zu berücksichtigen. Bei Bedarf kann die*der CISO die individuelle Planung unterstützen, um eine ausreichende Beachtung sicherzustellen.

6.2 Chief Information Security Officer

Die*der Chief Information Security Officer (CISO), oft auch Informationssicherheitsbeauftragte*r genannt, leitet die Stabsstelle Informationssicherheit. Sie*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.

Um 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. Die 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.

---

[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.

Im Verantwortungsbereich der*des CISO liegen dabei insbesondere die organisatorischen Aspekte der Informationssicherheit. Darunter fallen unter anderem das Steuern des Informationssicherheitsprozesses, Beratungsaufgaben, die Planung und Umsetzung von Awareness- und Schulungsmaßnahmen sowie die Abwicklung von Informationssicherheitsvorfällen.

Außerdem erstellt und aktualisiert die*der CISO die Informationssicherheitsleitlinie und die Informationssicherheitsstrategie, die anschließend dem Rektorat als Entwurf zur Verabschiedung vorgelegt werden. Die Erstellung der universitätsweiten Informationssicherheitsrichtlinien wird durch sie*ihn koordiniert und unterstützt. Die konkrete Erstellung einer Richtlinie findet in Abstimmung mit der*dem CISO durch die jeweiligen verantwortlichen Personen und Einrichtungen statt. Die erstellten Dokumente werden durch die*den CISO in Abstimmung mit dem Lenkungsausschuss für Informationssicherheit dem Rektorat zur Verabschiedung und Freigabe vorgelegt.

Mindestens einmal jährlich berichtet die*der CISO den aktuellen Stand der Informationssicherheit an der Universität direkt an das Rektorat.

Mögliche Interessenskonflikte müssen bei der Auswahl der*des CISO vermieden werden. Insbesondere darf die*der CISO keine weiteren Rollen wahrnehmen, die zu solchen Konflikten führen können. Dies schließt unter anderem die Rolle der*des Chief Information Officer (CIO) sowie der Leitung der Universitäts-IT aus.

Damit die*der CISO ihre*seine Funktion adäquat wahrnehmen kann, muss sie*er unabhängig sein. Das bedeutet, dass Vorgesetzte keinen Einfluss auf Gutachten oder Bewertungen der Informationssicherheit nehmen dürfen. Zur Gewährleistung dieser Unabhängigkeit sind fachliche, disziplinarische und finanzielle Aspekte zu berücksichtigen.

6.3 Rektorat

Das Rektorat trägt die Verantwortung für die Informationssicherheit an der Universität Mannheim. Es stellt sicher, dass Informationssicherheit, entsprechend dieser Leitlinie, an der Universität Mannheim realisiert, erhalten und weiterentwickelt wird.

Das Rektorat empfängt die Berichte der*des CISO. Der 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.

Die Informationssicherheitsleitlinie und die Informationssicherheitsstrategie werden durch das Rektorat verabschiedet und freigegeben. Auch universitätsweite Informationssicherheitsrichtlinien werden durch das Rektorat freigegeben. Die Befugnis zur Freigabe einer Richtlinie kann an andere Stellen oder Rollen delegiert werden.

Das Rektorat ist dafür verantwortlich, dass die Ressourcen für die Umsetzung und den Erhalt der Informationssicherheit verfügbar sind. Der*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

Aufgabe 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. Die Ausarbeitung der einzelnen Vorlagen für das Rektorat obliegt den für die jeweilige Maßnahme verantwortlichen Einrichtungen bzw. Personen.

Die Mitglieder des Lenkungsausschusses für Informationssicherheit sind kraft Amts:

- 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

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

7 Kooperationen

Da 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. So können, trotz lokaler Unterschiede der Hochschulen, Synergien genutzt werden. Dies soll durch bwInfoSec, den Kooperationsverbund für Informationssicherheit der Universitäten und Hochschulen in Baden-Württemberg, zusätzlich unterstützt werden. Die*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. Auch über den Kooperationsverbund und die Landesgrenzen hinaus soll die*der CISO sich kontinuierlich mit anderen Hochschulen und Universitäten austauschen.

8 Inkrafttreten

Für Beschäftigte gilt die Informationssicherheitsleitlinie ab dem Tag nach der Bekanntmachung. Sie ist von ihnen unverzüglich und somit so schnell, wie subjektiv zumutbar, einzuhalten.