IT Sicherheitsleitlinie

der Johannes Gutenberg-Universität Mainz

vom 28.04.2025

JOHANNES GUTENBERG UNIVERSITÄT MAINZ

JG|U

IT Sicherheitsleitlinie
der Johannes Gutenberg-Universität Mainz
vom 28. April 2025

Inhaltsübersicht

Präambel

Diese Leitlinie richtet sich an alle Mitglieder und Gäste der Johannes Gutenberg-Universität Mainz (JGU), die Geräte gleich welcher Art und Funktion an Netzwerken der JGU betreiben oder nutzen. Sie legt grundsätzliche Zuständigkeiten und Grundprinzipien im Bereich der IT-Sicherheit fest. Die Leitlinie wird durch zukünftige Betriebsregeln ergänzt, welche Details für den Betrieb von Geräten wie z. B. Druckern, Multimediageräten, Webservern, mobilen Endgeräten und anderen regeln.

Für die JGU ist die Informations- und Kommunikationstechnik von zentraler Bedeutung für die Aufgabenerfüllung in Forschung und Lehre sowie der Verwaltung. Das Spektrum der IT-Anwendungen umfasst den Betrieb von Anlagen, die Durchführung von Versuchen und Experimenten, wissenschaftliche Anwendungen und Simulationen, die Lehre, Online-prüfungen, die Arbeit in der Verwaltung sowie den Zentralen Einrichtungen und die Kommunikation mit externen Partnern und Auftraggebern.

Die Sicherheit in der Informationstechnik sowie die Einhaltung der datenschutzrechtlichen und weiteren gesetzlichen Bestimmungen sind eine grundlegende Voraussetzung für eine funk-tionsfähige Universität. Sie zu gewährleisten ist Aufgabe aller Einrichtungen der Universität und der Nutzenden der IT-Infrastruktur sowie der IT-Systeme.

Die IT-Sicherheit an der JGU orientiert sich an den jeweils aktuellen Richtlinien zum IT-Grund-schutz, veröffentlicht im IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit der Informationstechnik (BSI).

§ 1
Geltungsbereich

Die IT-Sicherheitsleitlinie gilt für alle Personen und Institutionen, die IT-Infrastruktur, Netz-werke und daran angeschlossene IT-Systeme der JGU an beliebigen Standorten der JGU nutzen oder selbst IT-Systeme in diesem Umfeld betreiben.

§ 2
Begriffsbestimmungen

Die vorliegende Leitlinie verwendet folgende Definitionen:

1. Grundwerte der Informationssicherheit

Die Grundwerte der Informationssicherheit sind die Vertraulichkeit, Integrität und Verfügbarkeit jeder Art von Daten.

Im Rahmen von Forschung, Lehre und Verwaltung, beispielsweise bei der Dokumentation von Forschungsprojekten, beim Umgang mit Forschungsdaten, der Erstellung wissenschaftlicher Arbeiten sowie der Erteilung von qualifizierten Leistungsnachweisen oder Zeugnissen, sind an der JGU weitere Grundwerte zu beachten:

a) Authentizität,
b) Verbindlichkeit,
c) Zuverlässigkeit und
d) Nichtabstreitbarkeit.

2. IT-Sicherheit

IT-Sicherheit beschreibt die Einhaltung der unter 1. definierten Grundwerte auf allen IT-Systemen und bei allen Prozessen der JGU, die Daten verarbeiten. Dazu zählen alle aktiven Komponenten des Netzwerks, alle Systeme, auf denen Daten gespeichert und verarbeitet werden, alle Verfahren, welche Daten erfassen, verarbeiten und speichern sowie alle Geräte, mit denen der Zugriff auf Daten möglich ist, und die dazugehörigen organisatorischen und baulichen Rahmenbedingungen.

3. Vertraulichkeit

Der Zugriff und die Nutzung von Daten jeglicher Art darf ausschließlich durch berechtigte Personen in definierter und zulässiger Weise erfolgen.

4. Integrität

Die Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf Daten angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf Informationen angewendet. Der Begriff Information wird dabei für Daten verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. die Autorschaft oder der Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zur Autorschaft verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.

5. Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

6. IT-Infrastruktur

Beim IT-Grundschutz werden unter Infrastruktur die für die Informationsverarbeitung und die IT genutzten Gebäude, Räume, Energieversorgung, Klimatisierung und die Verkabelung verstanden. Die eigentlichen IT-Systeme und Netzwerksysteme gehören nicht dazu.

7. IT-System

Die funktionelle Einheit aus Hard- und Software, die Daten erhebt, erfasst, aufbereitet, nutzt, speichert, übermittelt, programmgesteuert verarbeitet, intern darstellt, ausgibt und wiedergewinnt.

8. IT-Sicherheitsprozess

Die Gesamtheit der Verfahren, die das Ziel haben, IT-Sicherheit in alle Abläufe der Universität zu integrieren, um eine konstante Weiterentwicklung und Verbesserung der IT-Sicherheit zu gewährleisten.

§ 3
Grundprinzipien des Betriebs von IT-Systemen an der JGU

Für den Betrieb von Geräten an der JGU gelten folgende Prinzipien:

1. Mitglieder sowie Gäste der JGU erhalten Zugriff auf IT-Ressourcen, für die ein begründeter Bedarf besteht, wenn dieser Zugriff angemessen und sicher zu realisieren ist.
2. Mitglieder sowie Gäste der JGU dürfen eigene IT-Systeme an der JGU betreiben und erhalten für diese Geräte einen den Sicherheitsanforderungen der JGU entsprechenden Netzwerkanschluss mit Zugang zum Internet.
3. Mitarbeitende der JGU dürfen unter folgenden Bedingungen Netzwerkdienste auf eigenen IT-Systemen anbieten:

    a) Sie müssen über ausreichende, sachgerechte, aktuelle Kenntnisse sowohl über den Betrieb des IT-Systems als auch über IT-Sicherheit verfügen.
    b) Für das Anbieten von Netzwerkdiensten über das eigene Netzwerksegment hinaus muss ein begründeter Bedarf bestehen.
    c) Durch den Betrieb von IT-Systemen darf die Sicherheit der JGU IT-Infrastruktur und anderer IT-Systeme nicht beeinträchtigt werden.
    d) Zentrale Sicherheitsmaßnahmen, z. B. Firewalls oder Zugangs- und Zugriffsbeschränkungen, dürfen nicht umgangen werden.
4. Die Verantwortlichkeit für IT-Sicherheit folgt grundsätzlich den Zuständigkeiten für IT-Systeme, d. h. jeder oder jede, der oder die ein IT-System im Netzwerk der JGU betreibt, ist über die gesamte Lebenszeit des Systems für den ordnungsgemäßen und sicheren Betrieb bis zur Stilllegung und fachgerechten Entsorgung verantwortlich.
5. Ereignisse, die die IT-Sicherheit beeinträchtigen könnten, müssen unverzüglich an das ZDV gemeldet werden. Das ZDV informiert umgehend das IT-Sicherheitsboard.

§ 4
Beteiligte am IT-Sicherheitsprozess und deren Aufgaben

1. Präsidium

Die Gesamtverantwortung für die Gewährleistung der IT-Sicherheit und die Einhaltung des IT-Sicherheitsprozesses an der JGU liegt im Präsidium. Der Chief Information Officer (CIO) nimmt im Namen des Präsidiums die die Universität in ihrer Gesamtheit betreffenden Koordinierungsaufgaben im Bereich IT-Sicherheit wahr. In dieser Tätigkeit wird der CIO durch das IT-Sicherheitsboard unterstützt.

2. Senatsausschuss für Informationstechnologie und Digitale Prozesse

Der Senatsausschuss erarbeitet für den Bereich Informations- und Kommunikationstechnologien strategische Vorschläge als Entscheidungsgrundlage für den Senat. Ergebnisse werden gegebenenfalls zur Genehmigung bzw. Inkraftsetzung an das Präsidium weitergeleitet.

3. IT-Sicherheitsboard (IT-SB)

Das IT-Sicherheitsboard, IT-SB, wird vom CIO geleitet. Er wird in der Geschäftsführung von dem oder der Informationssicherheitsbeauftragten unterstützt, der oder die Mitglied des IT-SB ist. Die weiteren Mitglieder des Boards werden durch das Präsidium auf Vorschlag des CIO ernannt. Die Mitglieder des Boards zeichnen sich durch Erfahrung und Wissen auf dem Gebiet der IT-Sicherheit aus. Im IT-Sicherheitsboard sollen dabei neben dem CIO und Vertreterinnen und Vertretern des ZDV auch Vertreterinnen und Vertreter der Fachbereiche und IT-Sicherheitsexpertinnen oder Sicherheitsexperten von externen, kooperierenden Einrichtungen vertreten sein.

Die Aufgabe des IT-SB ist die Wahrnehmung der Aufgaben eines IT-Sicherheitsbeauftragten. Es ist verantwortlich für die Analyse und Verbesserung der IT-Sicherheit der JGU, die Beratung von Entscheidungsträgern der JGU, das Erstellen von Berichten zum Stand der IT-Sicherheit und die Bewertung von Berichten des CERT (§ 4 Nr.4) zu Sicherheitsvorfällen.
Es hat die Aufgabe, die IT-Sicherheitsleitlinie, die Betriebsregeln und die Wirksamkeit der bisherigen Organisationsform sowie der Maßnahmen und Prozesse für IT-Sicherheit kontinuierlich zu überprüfen und weiterzuentwickeln. Hierüber berichtet es dem Präsidium mindestens alle zwei Jahre.
Alle JGU-internen Angehörigen des IT-SB können auch als Informationssicherheitsbeauftragte der JGU fungieren.
In ihren Aufgaben bezüglich der IT-Sicherheit sind die Mitglieder des IT-SB nur an Weisungen des Präsidiums gebunden.

Die Mitglieder des IT-SB haben ein Vorschlagsrecht. Das Vorschlagsrecht dient dazu, eigene Vorschläge bezüglich der IT-Sicherheit an alle unter § 4 genannten Beteiligten und Gremien sowie an Nutzerinnen und Nutzer zu richten. Das IT-SB ist bei allen Projekten, die deutliche Auswirkungen auf die Sicherheitsaspekte der Informationsverarbeitung haben, zu informieren.

4. Krisenmanagement-Team IT-Sicherheit (Computer Emergency Response Team - CERT)

Aufgabe des Krisenmanagement-Teams IT-Sicherheit, CERT, ist die Steuerung und Koordination aller Maßnahmen im Rahmen von IT-Sicherheitsvorfällen an der JGU; es tritt in Aktion, sobald eines seiner Mitglieder einen IT-Sicherheitsvorfall identifiziert. Das Kernteam des CERT besteht aus dem CIO, dem Datenschutzbeauftragten, der technischen Leitung des ZDV sowie weiteren Mitarbeitenden des ZDV, welche von der technischen Leitung des ZDV benannt werden. Die Mitglieder des Kernteams können bei Bedarf Dritte in das CERT einbinden.
Das CERT berichtet in der Person des CIO anlassbezogen den anderen Mitgliedern des Präsidiums.

5. Leitung des Zentrums für Datenverarbeitung (ZDV)

Die technische Leitung des ZDV ist verantwortlich für die Sicherheit der vom ZDV betriebenen IT-Infrastruktur und IT-Systeme sowie des Netzes der JGU und verantwortet die Dokumentation der realisierten Sicherheitsmaßnahmen.

6. Verantwortliche für IT-Systeme

Jeder oder jede, der oder die an der JGU ein IT-System betreibt, ist berechtigt, neben den hochschulweiten IT-Sicherheitsmaßnahmen, eigene weiterführende Maßnahmen zu treffen. Bei möglichen Auswirkungen auf die IT-Infrastruktur und IT-Systeme der Universität muss eine Abstimmung mit dem ZDV erfolgen. Getroffene Maßnahmen sind zu dokumentieren.

§ 5
Gefahrenintervention

Das ZDV ist berechtigt, bei Gefahr im Verzug unmittelbar notwendige Abwehrmaßnahmen vorzunehmen. Wenn notwendig, werden die Abwehrmaßnahmen durch das CERT koordiniert. Bei den zu treffenden Maßnahmen ist der Grundsatz der Verhältnismäßigkeit der Mittel zu wahren. Die Maßnahmen sollen so erfolgen, dass die betroffenen Nutzende - wenn irgend möglich - bereits vorher in Kenntnis gesetzt werden. Betroffene Nutzende (soweit ermittelbar), die Leitung der betroffenen Einrichtung und die Geschäftsführung des IT-SB sind unverzüglich über den Vorfall und die getroffenen Maßnahmen zu informieren.

Wird ein Vorfall von einem oder einer Verantwortlichen für ein IT-System als potenziell die IT-Sicherheit gefährdendes Ereignis eingestuft, ist dieser oder diese verpflichtet, unverzüglich geeignete Abwehrmaßnahmen zu treffen und das ZDV von dem Ereignis und den getroffenen Maßnahmen in Kenntnis zu setzen.

§ 6
Vorbeugende Maßnahmen

Für die Sicherstellung der IT-Sicherheit sind vorbeugende Maßnahmen notwendig. Mit geeigneten technischen und organisatorischen Maßnahmen sollen Gefährdungsrisiken erfasst und eingedämmt sowie Angriffe auf die IT-Sicherheit frühzeitig erkannt werden.

Das IT-SB und das ZDV können vorbeugende Maßnahmen vorschlagen. Die Durchführung vorbeugender Maßnahmen obliegt dem jeweils zuständigen IT-Systembetreiber. Die Entscheidung über die Umsetzung bereichsübergreifender Maßnahmen obliegt dem Präsidium.

§ 7
Inkrafttreten

Diese IT-Sicherheitsleitlinie der JGU tritt am Tag nach ihrer Veröffentlichung in Kraft. Gleichzeitig tritt die IT-Sicherheitsleitlinie der JGU vom 07.10.2021 außer Kraft.

Mainz, den 16.06.2025

Gez.

Universitätsprofessor
Dr. Georg Krausch
- Präsident -