Leitlinie zur Informationssicherheit der Hochschule der Medien Stuttgart (Informationssicherheitsleitlinie)

Dokumenteneigenschaften

Verantwortung	Informationssicherheitsbeauftragte/r
Klassifizierung	~~Öffentlich~~ / Intern / ~~Vertraulich~~ / ~~Streng Vertraulich~~ TLP Green
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	11/2025
Dateiname	

Dokumentenhistorie

Version	Änderung	Datum	Autor
0.1	Erster Entwurf erstellt aus Vorlage „RecPlast GmbH“ des BSI	26.10.2021	Roland Schmitz
0.7	Finale Version nach Durchsicht des Justiziariats	6.04.2022	Barbara Richter, Peter Marquardt
1.0	Neue Version nach Durchsicht durch den ISB - ENTWURF	22.03.2023	Matthias Menze
1.1	Korrekturen in den Kap. 6.2 & 6.3	11.08.2023	Matthias Menze
2.0	Durchsicht durch das ISM-Team	14.12.2023	Matthias Menze
2.1	Schlussredaktion	18.01.2024	Matthias Menze
2.2	Korrekturen ISM-Team	11.03.2024	Matthias Menze
2.3	Abschnitt 3 überarbeitet	25.03.2024	Matthias Menze
2.4	Definition ISMS eingefügt, kleine inhaltliche Änderungen	26.04.2024	Matthias Menze
2.5	Klassifizierung eingefügt, Abschnitt 6.3 finalisiert	18.11.1024	Matthias Menze

Inhalt

1 Präambel

Die Hochschule der Medien Stuttgart (HdM) ist eine staatliche Hochschule für angewandte Wissenschaften (HAW) des Landes Baden-Württemberg, die Spezialisten rund um die Medien ausbildet.

Die HdM etabliert ein Informationssicherheitsmanagementsystem (ISMS), das dem Standard 200-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI), sowie der ISO/IEC 27001 genügt.

Das ISMS in seiner Funktion als Managementsystem legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, einsetzt, durchführt, überwacht und verbessert).
Einer der zentralen Bestandteile des ISMS ist die hier vorliegende Leitlinie zur Informationssicherheit der Hochschule der Medien Stuttgart (Informationssicherheitsleitlinie).
Sie ist abgeleitet aus den Zielen der HdM im Bereich Lehre und Forschung, wie sie unter anderem im Leitbild Lehre der HdM dargelegt sind, und den Sicherheitsanforderungen der Prozesse, mit denen diese Ziele erreicht werden.

Die Informationssicherheitsleitlinie gilt für alle Mitglieder, Angehörige und Nutzenden der Infrastruktur der HdM, das heißt z. B. Beschäftigte, Studierende sowie externe Personen und wird deshalb auch allen zur Kenntnis gegeben. Sie dient nicht nur einem sicheren, sondern auch einem reibungslosen und effizienten Ablauf der IT-Prozesse und der weiteren Geschäftsprozesse an der HdM.

2 Kontext

2.1 Einleitung

Die hier vorliegende Informationssicherheitsleitlinie beschreibt allgemeinverständlich, was Informationssicherheit ist und welche Bedeutung sie für die HdM hat. Das Dokument zeigt auf, wie Informationssicherheit an der HdM umgesetzt wird, indem das zu erreichende Mindest-Sicherheitsniveau beschrieben wird sowie die angestrebten Informationssicherheitsziele und die verfolgte Informationssicherheitsstrategie dargestellt werden.

Die Informationssicherheitsleitlinie ist Bestandteil eines hierarchisch abgestuften Regelwerks. Ganz bewusst wurde diese Leitlinie frei gehalten von konkreten Regelungen oder Handlungsanweisungen. Die Leitlinie wird einer jährlichen Revision unterzogen.

Ergänzt wird die Informationssicherheitsleitlinie durch weiterführende Regelungen wie z.B. Sicherheitsrichtlinien, die im ISMS zusammengefasst werden. Das ISMS gibt den Mitgliedern und Angehörigen sowie Nutzenden der Infrastruktur der HdM einen Handlungsrahmen vor, mit dem die definierten Ziele der HdM im Bereich der Informationssicherheit erreicht werden können.

2.2 Dokumente der Informationssicherheit

Im Folgenden werden die drei zentralen Dokumente im Bereich der Informationssicherheit in Anlehnung an die Definitionen des BSI abgegrenzt.

- **Informationssicherheitsleitlinie:** Die Informationssicherheitsleitlinie beschreibt allgemeinverständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der HdM hergestellt werden soll. Sie beinhaltet die angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Die Informationssicherheitsleitlinie beschreibt auch das angestrebte Sicherheitsniveau in der HdM.
- **Informationssicherheitskonzept:** Zum Erreichen der in der Informationssicherheitsleitlinie festgeschriebenen Ziele wird ein Sicherheitskonzept entworfen und umgesetzt. Dieses Sicherheitskonzept ist das zentrale Dokument im Informationssicherheitsprozess der HdM. Es dient zur Umsetzung der definierten Informationsstrategie und beschreibt die geplante Vorgehensweise, um die gesetzten Sicherheitsziele zu erreichen. Das Sicherheitskonzept wird in regelmäßigen Abständen einer Qualitätskontrolle unterzogen und entsprechend aktualisiert.
- **Informationssicherheitsrichtlinien:** Sicherheitsrichtlinien beschreiben konkrete Maßnahmen zum Umgang mit Applikationen, Netzwerkkomponenten und IT-Systemen, die Informationen verarbeiten. Ebenfalls werden Zutrittsregeln für Räumlichkeiten und Einrichtungen, Zugangsregeln für IT-Systeme/Komponenten und Zugriffsregeln auf Informationen durch Sicherheitsrichtlinien festgehalten. Die Einhaltung und Umsetzung dieser Richtlinien sind für alle Personen verbindlich. Sicherheitsrichtlinien können einen hochschulweiten Geltungsbereich haben. In Abhängigkeit von Umsetzbarkeit und Bedarf können aber auch fakultäts- und/oder zielgruppenspezifische Vorgaben formuliert werden.

2.3 Grundlegende Ziele der Informationssicherheit

Aufgabe der Informationssicherheit ist der angemessene Schutz der folgenden drei Grundwerte:

- **Integrität:**
  Mit diesem Begriff wird die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen bezeichnet. Bei intakter Integrität sind Daten vollständig und unverändert. Eventuell zugehörige Attribute wurden nicht unerlaubt manipuliert.
- **Verfügbarkeit:**
  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.
- **Vertraulichkeit:**
  Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen wie auch der Zutritt zu Räumlichkeiten dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Um zu gewährleisten, dass weitere Grundwerte gewahrt bleiben, werden personenbezogene Daten durch den Datenschutz geschützt.

2.4 Geltungsbereich

Der Geltungsbereich dieser Informationssicherheitsleitlinie ist der Geltungsbereich des ISMS, wie in der Strukturanalyse beschrieben.

Diese Leitlinie richtet sich an alle Mitglieder und Angehörigen wie auch alle Nutzenden der Infrastruktur der HdM. Hierzu zählen auch die Beschäftigten von beauftragten Dienstleistungsunternehmen, Kooperationspartnern, Instituten und Nutzenden bei allen weiteren Einrichtungen, die an das Hochschulnetz angeschlossen sind oder dessen Netzinfrastruktur, IT-Dienste und/oder den Internetzugang der Hochschule nutzen.

2.5 Ansprechperson

Die Ansprechperson zu allen Fragen dieser Richtlinie ist der/die Informationssicherheitsbeauftragte (ISB) der HdM.

2.6 Verantwortlichkeiten

Diese Informationssicherheitsleitlinie wird vom Rektor bzw. der Rektorin der HdM freigegeben.

3 Stellenwert der Informationstechnologie und Informationssicherheit

Die Informationssicherheit stellt für die HdM ein wichtiges Qualitätsmerkmal derDatenverarbeitung dar, da alle wesentlichen strategischen und operativen Prozesse an der HdM durch Informationstechnologie (IT) maßgeblich unterstützt werden.

Die dauerhafte Verfügbarkeit von relevanten Informationen und der Schutz von Vertraulichkeit und Integrität von sensiblen Hochschul- und personenbezogenen Daten - hierzu gehören Personaldaten

ebenso wie Daten von Studierenden und Forschungsunterlagen - ist entscheidend für die Erfüllung des Bildungsauftrages der HdM. Das Risiko für einen unberechtigten Zugriff und vor unerlaubter Änderung gilt es, auf ein akzeptables Maß zu reduzieren. Das bedeutet insbesondere, dass die Wahrscheinlichkeit eines Schadensfalls mit hohen finanziellen Auswirkungen und insbesondere immateriellen Folgen in Form von Imageschäden für die HdM so weit wie möglich verringert werden muss. Der gute Ruf und das Ansehen der HdM bei Bewerber und Bewerberinnen, in der allgemeinen Öffentlichkeit, bei Forschungs- sowie Praxispartnern muss durch die Informationssicherheit geschützt werden.

Die Sicherstellung der Verfügbarkeit von Daten und IT-Systemen in allen Bereichen der Forschung, Lehre und Verwaltung ist ebenso von Bedeutung und soll durch geeignete Schutzmaßnahmen sicherstellen, dass eventuelle Ausfallzeiten noch toleriert werden können.

Beeinträchtigungen hinsichtlich der Verfügbarkeit der hochschuleigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen.

Die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, Anwendungen und IT-Systeme werden nicht nur durch externe Angreifende bedroht, sondern auch durch interne Angreifende mit möglichem Wissen über Schwachstellen.

4 Ziele der HdM

Die Aufgaben in Lehre und Forschung sowie Administration und Verwaltung an der HdM werden, wie in Abschnitt 3 beschrieben, zunehmend von der Nutzung der Informationstechnologie als modernes Lehr-, Informations- und Kommunikationsmedium bestimmt. Daher verfolgt die HdM mit Fokus auf die Bewahrung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität der Informationen folgende weiterführende Ziele im Bereich Informationssicherheit:

Einhaltung von Gesetzen und Vorschriften:

Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für die HdM relevanten Gesetze, Vorschriften und vertragliche Verpflichtungen eingehalten werden.

Die wichtigsten zu beachtenden Vorgaben und Regelungen sind dabei:

- Landeshochschulgesetz (LHG)
- Landesdatenschutzgesetz (LDSG)
- EU-Datenschutz-Grundverordnung (EU-DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Allgemeines Gleichbehandlungsgesetz (AGG)
- Datenschutz-Verordnung der Hochschule der Medien Stuttgart
- einschlägige Verwaltungsvorschriften des Landes Baden-Württemberg, z.B. VwV Informationssicherheit

Die Informationssicherheit dient der Umsetzung und Einhaltung von gesetzlich geforderten Maßnahmen.

Wahrung von Persönlichkeitsrechten:

Im Zuge der Erfüllung ihres Bildungs- und Forschungsauftrages erhebt und verarbeitet die HdM Daten, die die Persönlichkeitsrechte der Betroffenen (Studierende und Beschäftigten) berühren. Die

Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten sind zu schützen, sodass die Persönlichkeitsrechte der betroffenen Personen stets gewahrt bleiben und die rechtlichen Rahmenbedingungen stets eingehalten werden.

Funktionale Aufgabenerledigung:

Die Informationstechnik muss so betrieben werden, dass die für die Erfüllung des Bildungsauftrags erforderlichen Informationen hinreichend schnell verfügbar sind. Ausfälle, die zu langen Verzögerungen bei der Erfüllung dieser Aufgaben führen, sind nicht tolerierbar.

Informationssicherheit unterstützt damit auch eine funktionale Aufgabenerledigung.

Vermeidung von Ansehensverlust bzw. Imageschaden:

Ein negatives Image für die HdM durch Informationssicherheitsvorfälle muss verhindert werden.

Ein Ansehensverlust führt auf längere Sicht zu weniger Studienbewerberinnen sowie Studienbewerber und damit auch zu weniger staatlichen Mitteln. Die Folge wäre eine geringere Qualität der Lehre durch weniger angebotene Lehrveranstaltungen und eine schlechtere personelle Ausstattung. Informationssicherheit vermeidet Ansehensverlust sowie Imageschaden der HdM und trägt somit zu einer hohen Qualität der Lehre bei.

Vermeidung materiellen Schadens:

Unmittelbare oder mittelbare finanzielle Schäden können durch den Verlust der Vertraulichkeit schutzbedürftiger Daten, die Veränderung von Daten oder den Ausfall einer IT-Anwendung oder eines IT-Systems entstehen. Informationssicherheit wirkt damit auch materiellen Schäden entgegen.

Schaffung eines Bewusstseins für Informationssicherheit:

Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen (TOMs) erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Beschäftigten diemöglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Qualifizierungsmaßnahmen zur Informationssicherheit unterstützen hierbei und werden daher allen Hochschulmitgliedern und -angehörigen angeboten werden.

Kontinuierliche Verbesserung:

Die Informationssicherheit und ihre Prozesse werden kontinuierlich verbessert.

5 Sicherheitsniveau und Sicherheitsstrategie

An der HdM wird im Rahmen der Basis-Absicherung ein Sicherheitsniveau angestrebt, das mindestens für den normalen Schutzbedarf (gemäß BSI) hochschulrelevanter Informationen angemessen und ausreichend ist. Die hierzu umzusetzenden Maßnahmen liefern einerseits einen soliden Grundschutz für alle Informationen und Daten und die verbundenen Komponenten, dienen aber andererseits auch als Basis für weitergehende Aktivitäten.

Bereiche mit hohem Schutzbedarf werden nach den Methoden der Kern-Absicherung (nach BSI-Grundschutz) geschützt.

Die Informationssicherheitsstrategie wird durch das Rektorat der HdM festgelegt und niedergeschrieben.

Dabei arbeitet der bzw. die Informationssicherheitsbeauftragte (ISB) sowie das Informationssicherheits-management-Team (ISM-Team) zu. Die HdM orientiert sich bei der Gestaltung von Informationssicherheit an den vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeiteten Regelungen und der Methodik des IT-Grundschutzes. Eine hochschulweite Zertifizierung wird zurzeit nicht angestrebt.

Um das definierte Sicherheitsniveau der HdM aufrecht zu erhalten, ist eine fortlaufende Kontrolle und Verbesserung der implementierten Sicherheitsmaßnahmen, Dokumente und des festgelegten Informationssicherheitsprozesses zwingend erforderlich. Dazu findet in der Regel jährlich, mindestens aber alle zwei Jahre, eine Erfolgskontrolle und Bewertung durch das Rektorat, die IT-Leitung und den/der ISB statt. Die Informationssicherheitsleitlinie wird durch den ISB ebenfalls in der Regel jährlich, mindestens aber alle zwei Jahre, überprüft und aktualisiert. Der/die ISB wird dabei durch das Informationssicherheitsmanagement-Team unterstützt.

6 Organisation des Informationssicherheitsmanagementsystems

Grundsätzlich sind folgende Verantwortlichkeiten innerhalb des ISMS definiert:

6.1 Rektorat

Das Rektorat beschließt auf Vorschlag des/der Informationssicherheitsbeauftragten (ISB) die Informationssicherheitsleitlinie. Der/die Rektor/in unterzeichnet die Informationssicherheitsleitlinie.

Das Rektorat ist dafür verantwortlich, sicherzustellen, dass das ISMS entsprechend dieser Leitlinie umgesetzt und aktualisiert wird und dass die notwendigen Ressourcen zur Verfügung stehen. Der IT-Leitung und dem/der ISB werden vom Rektorat ausreichende finanzielle, personelle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden, zu informieren und die vom Rektorat festgelegten Sicherheitsziele zu erreichen.

Das Rektorat muss das ISMS mindestens einmal jährlich überprüfen (bzw. immer im Falle von erheblichen Änderungen) und freigeben. Zweck dieser Überprüfung durch das Rektorat ist der Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS.

Die Gesamtverantwortung für die ordnungsgemäße und sichere Aufgabenerfüllung (und damit die Informationssicherheit) verbleibt beim Rektorat.

6.2 Informationssicherheitsbeauftragte/r (ISB)

Der/die Informationssicherheitsbeauftragte (ISB) ist für die Koordination des Betriebs des ISMS verantwortlich, sowiefür die Berichterstattung über dessen Leistungsfähigkeit. Er/sie ist des Weiteren für die Koordination bzw. Umsetzung von Informationssicherheitstrainings und -programmen zur Bewusstseinsbildung (Awareness) für die Nutzenden der Infrastruktur verantwortlich. Der/die ISB definiert, welche sich auf Informationssicherheit beziehenden Informationen durch wen und wann kommuniziert werden. Dies gilt sowohl für interne als auch externe Bereiche.

Er/sie koordiniert die Aufstellung und Implementierung des Plans für Training und Awareness, dem alle Personen unterliegen, die eine Rolle im ISMS innehaben.

Der/die ISB ist verantwortlich für die Definition der Behandlung von Sicherheitsvorfällen.

Die Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten bedarf einer Freigabe durch den/die ISB und das ISM-Team. Dabei muss besonderes Augenmerk darauf gerichtet werden, dass durch den Einsatz der neuen Anwendungen, Verfahren und Komponenten die Risiken hinsichtlich der Informationssicherheit (Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit)

nicht erhöht, sondern möglichst minimiert werden.

Der/die ISB berät das Rektorat, die Fakultäten und die Verwaltung der HdM in Fragen der Informationssicherheit und arbeitet mit der IT-Leitung zusammen. Er/sie beobachtet laufend die technischen und organisatorischen Fortentwicklungen im Bereich der Informationssicherheit und schlägt in Abstimmung mit der IT-Leitung die notwendigen Maßnahmen vor. Des Weiteren ist er/sie frühzeitig in alle Projekte einzubinden, um sicherzustellen, dass bereits in der Planungsphase alle sicherheitsrelevanten Aspekte berücksichtigen werden.

6.3 IT-Leitung

Die zentrale Instanz für die operative IT-Sicherheit ist die Abteilung Core IT. Sie ist für den sicheren Betrieb der zentralen IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich. In Zusammenarbeit mit dem/der ISB bringt sie die für die Informationssicherheit spezifischen Aspekte und Anliegen ein und ist für die Umsetzung geeigneter Sicherheitsmaßnahmen zuständig. Für den sicheren Betrieb der an der HdM bestehenden dezentralen IT-Systeme sind die jeweiligen Zuständigen („IT-Beauftragte“) verantwortlich.

Die/der ISB wird frühzeitig in alle anstehenden IT-Projekte eingebunden. Für zentrale IT-Projekte stellt dies die Leitung der Core IT sicher, für dezentrale Projekte die Verantwortlichen der jeweiligen IT-Systeme. Darüber hinaus werden die Systembeauftragten für die an der HdM vorhandenen dezentralen IT-Systeme vor einer geplanten Einführung neuer Sicherheitsmaßnahmen und –richtlinien an der HdM im Rahmen des Arbeitskreises Informationssicherheit (siehe Abschnitt 6.4) informiert und in die Diskussion/Entscheidungsfindung mit einbezogen.

6.4 Informationssicherheitsmanagement-Team (ISM-Team)

Das Informationssicherheitsmanagement-Team (ISM-Team) setzt sich aus der/dem ISB als Vorsitzende/n, der/dem Datenschutzbeauftragten, eine Vertretung jeder Fakultät, der Technische Betriebsleitung, der IT-Leitung und gegebenenfalls weiteren fachkundigen Mitarbeiter und Mitarbeiterinnen zusammen. Werden weitere fachkundigen Mitarbeiter und Mitarbeiterinnen vom/ von der Vorsitzenden benannt, so bedarf es der vorherigen Zustimmung des Rektors oder der Rektorin. Die Benennung erfolgt für vier Jahre und kann mehrmals wiederholt werden. Das Informations-sicherheitsmanagement-Team hält regelmäßige Treffen ab.

Das ISM-Team plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung der Informationssicherheit an der HdM und berät den/die ISB. Weiterhin werden im ISM-Team Audits geplant und Sicherheitsvorfälle besprochen. Im ISM-Team werden auch die Dokumente des ISMS laufend überprüft und überarbeitet. Planungen und Änderungen in den Anwendungsbereichen sind stets im ISM-Team abzustimmen.

6.5 Mitglieder und Angehörige der HdM

Die Mitglieder und Angehörige der HdM sollen sich stets der Bedeutung der Informationssicherheit bewusst sein und aktiv an der Abwehr und Bekämpfung von materiellen und ideellen Schäden mitwirken. Sie sollen verantwortungsbewusst mit Informationssystemen und den darauf gespeicherten und dort verarbeiteten Daten umgehen und auf die Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit der gespeicherten Daten achten.

Erlangen Mitglieder oder Angehörige Kenntnis von Unregelmäßigkeiten, müssen sie diese unverzüglich den entsprechenden Stellen melden, üblicherweise dem/der ISB oder den Fachvorgesetzten. Es wird erwartet, dass jede/r Nutzer/in von IT-Systemen an der HdM die vorliegende Informationssicherheitsleitlinie kennt und beachtet. Hierzu wird die Informationssicherheitsleitlinie in geeigneter Form bekanntgegeben und darüber hinaus geeignete interne Schulungsmaßnahmen angeboten. Darüber hinaus sollen jede/r Nutzer/in geeignete Ressourcen zur Verfügung stehen, um die

Vorgaben der Leitlinie und des Sicherheitskonzepts umsetzen zu können.

6.6 Weitere Verantwortlichkeiten

Für alle Informationen, Prozesse, sowie die informationstechnischen Systeme und Infrastruktureinrichtungen werden Verantwortliche (Informations-, Prozess- und Systemeigentümer, Eigentümer von Zielobjekten) benannt. Diese sind dafür zuständig, den Schutzbedarf von Informationen und IT-Systemen einzuschätzen und darauf zu achten, dass die Beschäftigten dieser Bedeutung entsprechend handeln. Sie verwalten Zugriffsrechte und Autorisierungen in ihrem Zuständigkeitsbereich und sind gegenüber dem Rektorat rechenschaftspflichtig. Sie sind auch dafür verantwortlich, externen Dienstleistern und Kooperationspartnern die Vorgaben der HdM zur Informationssicherheit zur Kenntnis zu geben und deren Einhaltung zu überwachen.

7 Folgen von Zuwiderhandlungen

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können den Ruf der HdM gefährden, finanzielle Verluste bedeuten oder Beschäftigte und Studierende schädigen.

Verstöße gegen diese Informationssicherheitsleitlinie können deshalb zivilrechtliche, strafrechtliche, bei Beamten disziplinarische und bei Tarifbeschäftigten arbeitsrechtliche Folgen haben, sofern durch den Verstoß geltendes Recht verletzt wurde.

8 Weitere Maßnahmen

Ausgehend von der IT-Grundschutz-Methodik zur Einführung und Aufrechterhaltung eines ISMS wird ein Informationssicherheitskonzept und sonstige Regelungen wie z.B. Sicherheitsrichtlinien und technisch-organisatorische Maßnahmen erarbeitet, welche diese Leitlinie konkretisieren und gleichfalls gültig sind.

9 Inkrafttreten

Diese Informationssicherheitsleitlinie gilt ab dem 1. Dezember 2024. Gleichzeitig verliert die Leitlinie zur Informationssicherheit der Hochschule der Medien Stuttgart vom 1. Januar 2022, zuletzt geändert am 2. April 2022, ihre Gültigkeit.

Stuttgart, den 20.11.2024

Prof. Dr. Alexander W. Roos

Rektor Hochschule der Medien