HOCHSCHULE
DER MEDIEN

Leitlinie zur Informationssicherheit der Hochschule der Medien Stuttgart

Stand: 22.4.2022

Dokumenteneigenschaften

Verantwortung	Informationssicherheitsbeauftragte*r
Klassifizierung	internes Dokument
Gültigkeitszeit	Unbegrenzt
Überarbeitungsintervall	Jährlich
Nächste Überarbeitung	
Dateiname	

Dokumentenhistorie

Version	Änderung	Datum	Autor
0.1	Erster Entwurf erstellt aus Vorlage „RecPlast GmbH“ des BSI	26.10.2021	Roland Schmitz
0.2	Neue Version nach Kommentaren von Benjamin Binder	24.11.2021	Roland Schmitz
0.3	Neue Version nach Kommentaren von Sibylle Sowa	02.12.2021	Roland Schmitz
0.31,0.31a	Neue Version nach Kommentaren von Bettina Schwarzer (wurde im Kickoff vorgestellt)	06.12.2021	Roland Schmitz
0.4	Neue Version nach Kommentaren im und nach dem Kickoff-Meeting	20.12.2021	Roland Schmitz
0.41	Neue Version nach Kommentaren von Benjamin Binder	13.01.2022	Roland Schmitz
0.5, 0.5a	Im Arbeitskreis Informationssicherheit verabschiedete Version	03.02.2022, 07.02.2022	Roland Schmitz
0.6	Neue Version nach Durchsicht des Justiziariats	23.3.2022	Barbara Richter, Peter Marquardt
0.7	Finale Version nach Durchsicht des Justiziariats	6.4.2022	Barbara Richter, Peter Marquardt

Inhalt

1 **Präambel** 4

2 **Kontext** 5

2.1 Einleitung 5

2.2 Dokumente der Informationssicherheit 5

2.3 Grundlegende Ziele der Informationssicherheit 6

2.4 Geltungsbereich 6

2.5 Ansprechperson 6

2.6 Verantwortlichkeiten 6

3 **Stellenwert der Informationstechnologie und** 7

Informationssicherheit 7

4 **Ziele der HdM** 8

5 **Sicherheitsniveau und Sicherheitsstrategie** 9

6 **Organisation des Informationssicherheitsmanagementsystems** 10

6.1 Rektorat 10

6.2 Informationssicherheitsbeauftragte*r (ISB) 10

6.3 IT-Leitung 11

6.4 Arbeitskreis Informationssicherheit 11

6.5 Mitglieder und Angehörige der HdM 11

6.6 Weitere Verantwortlichkeiten 12

7 **Folgen von Zuwiderhandlungen** 12

8 **Weitere Maßnahmen** 12

9 **Inkrafttreten** 12

1 Präambel

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

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

Zentraler Bestandteil eines ISMS ist diese vorliegende Leitlinie zur Informationssicherheit. Sie ist abgeleitet aus den Zielen der HdM im Bereich Lehre und Forschung, wie sie z. B. im Leitbild Lehre der HdM dargelegt sind, und den Sicherheitsanforderungen der Prozesse, mit denen diese Ziele erreicht werden.

Die Leitlinie gilt für alle Mitglieder, Angehörige und Nutzenden der Infrastruktur der HdM, das heißt z. B. Mitarbeitende, Lehrende, Studierende sowie andere 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 an der HdM, der gleichzeitig auch die Persönlichkeitsrechte aller Betroffenen schützt.

2 Kontext

2.1 Einleitung

Die Hochschule der Medien (HdM) hat ein Informationssicherheitsmanagementsystem (ISMS) etabliert, das dem Regelwerk „IT-Grundschutz“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) genügt.

Das vorliegende Dokument ist die Leitlinie zur Informationssicherheit der HdM.

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

Die Leitlinie zur Informationssicherheit ist Bestandteil eines hierarchisch abgestuften Regelwerks. Ganz bewusst wurde diese Leitlinie frei gehalten von konkreten Regelungen oder Handlungsanweisungen, sondern hat eher einen allgemeinen Charakter. Sie soll im Gegensatz zu technischen Feinkonzepten oder organisatorischen Maßnahmen, welche einen dynamischen Charakter haben müssen, um auf aktuelle Gegebenheiten eingehen zu können, statisch sein und möglichst selten verändert werden.

Ergänzt wird die Sicherheitsleitlinie durch weiterführende Regelungen, die im ISMS zusammengefasst werden. Das ISMS gibt den Mitgliedern und Angehörigen und 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.

- **Leitlinie zur Informationssicherheit:** Die Leitlinie zur Informationssicherheit 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 Leitlinie zur Informationssicherheit beschreibt auch das angestrebte Sicherheitsniveau in der HdM.
- **Sicherheitskonzept:** Zum Erreichen der in der Leitlinie zur Informationssicherheit 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.
- **Sicherheitsrichtlinien:** 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 ist für alle Personen verbindlich. Sicherheitsrichtlinien können hochschulweiten Charakter haben. In Abhängigkeit von Umsetzbarkeit und Bedarf können aber auch fakultäts- oder zielgruppenspezifische Vorgaben formuliert werden.

2.3 Grundlegende Ziele der Informationssicherheit

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

- **Integritätsschutz:**
  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. Die Einhaltung weiterer Grundwerte wird für personenbezogene Daten durch den Datenschutz geprüft.

2.4 Geltungsbereich

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

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

2.5 Ansprechperson

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

2.6 Verantwortlichkeiten

Diese Leitlinie hat der Rektor der HdM in seiner Funktion als Vertreter der Hochschulleitung freigegeben.

3 Stellenwert der Informationstechnologie und Informationssicherheit

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.

Der Schutz von Vertraulichkeit und Integrität von sensiblen Hochschuldaten 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 immaterielle 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*innen, in der allgemeinen Öffentlichkeit, bei Forschungs- sowie Praxispartnern, muss durch die Informationssicherheit geschützt werden.

Der Schutz 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 Stillstandzeiten 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 interne 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 Bewahrung der Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität die folgenden weitergehenden 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.

Als wichtigste zu beachtende Rahmenbedingungen gelten dabei:

- Landeshochschulgesetz (LHG)
- Landesdatenschutzgesetz (LDSG)
- Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Allgemeines Gleichbehandlungsgesetz (AGG)
- Datenschutz-Verordnung der Hochschule der Medien Stuttgart

Informationssicherheit unterstützt damit auch die Einhaltung von Gesetzen und Vorschriften.

Wahrung von Persönlichkeitsrechten:

Im Zuge der Erfüllung ihres Bildungs- und Forschungsauftrages erhebt und verarbeitet die HdM Daten, die die Persönlichkeitsrechte der Betroffenen (Studierende, Lehrende und Mitarbeitenden) 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 Studienbewerber*innen 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 und 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 die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit können hierbei unterstützen, und sollten daher allen Beschäftigten angeboten werden.

Kontinuierliche Verbesserung:

Die HdM strebt die kontinuierliche Verbesserung ihrer Prozesse rund um dieInformationssicherheit an.

5 Sicherheitsniveau und Sicherheitsstrategie

An der HdM wird 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 Daten und die verbundenen Komponenten, dienen aber andererseits auch als Basis für weitergehende Aktivitäten. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der zu schützenden Ressourcen sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit

Hoch schutzbedürftige Informationen, IT-Systeme und Anwendungen usw. werden über diesen Grundschutz hinaus individuell analysiert und abgesichert.

Die Informationssicherheitsstrategie wird durch die Leitung der HdM festgelegt und niedergeschrieben. Dabei wird ihr von der bzw. vom Informationssicherheitsbeauftragten (ISB) sowie dem Arbeitskreis Informationssicherheit zugearbeitet. Die HdM orientiert sich bei der Gestaltung von Informationssicherheit am BSI und dessen 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 die Leitungsebene (Rektor, Leitung Campus IT, ISB) statt. Hierzu beauftragt der Rektor den ISB. Die Leitlinie zur Informationssicherheit wird durch den ISB ebenfalls in der Regel jährlich, mindestens aber alle zwei Jahre, überprüft und aktualisiert. Der ISB wird dabei durch den Arbeitskreis Informationssicherheit unterstützt.

6 Organisation des Informationssicherheitsmanagementsystems

Grundsätzlich sind folgende Verantwortlichkeiten innerhalb des ISMS definiert:

6.1 Rektorat

Das Rektorat als Hochschulleitung verabschiedet auf Vorschlag des/der Informationssicherheitsbeauftragten diese Informationssicherheitsleitlinie. Der/die Rektor*in unterzeichnet die Informationssicherheitsleitlinie.

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

Das Rektorat muss das ISMS mindestens einmal jährlich überprüfen (bzw. immer im Falle vonerheblichen Änderungen) und freigeben. Zweck dieser Überprüfung durch das Management 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)

Die/der Informationssicherheitsbeauftragte ist für die Koordination des Betriebs des ISMS verantwortlich, sowie für die Berichterstattung über dessen Leistungsfähigkeit. Sie oder er ist des Weiteren für die Koordination bzw. Umsetzung von Informationssicherheitstrainings und -programmen zur Bewusstseinsbildung (Awareness) für die Beschäftigten verantwortlich. Die/der ISB definiert, welche sich auf Informationssicherheit beziehenden Informationen durch wen und wann kommuniziert werden. Dies gilt sowohl für interne als auch externe Parteien.

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

Die Einführung neuer Anwendungen, Verfahren, Prozesse und Infrastrukturkomponenten bedarf einer Freigabe durch ISB. 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 werden.

Die/der ISB berät das Rektorat, die Fakultäten und die Verwaltung der HdM in Fragen der Informationssicherheit und arbeitet mit der IT-Leitung zusammen. Sie/er 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 sie bzw. er frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase alle sicherheitsrelevanten Aspekte berücksichtigen zu können.

6.3 IT-Leitung

Die zentrale Instanz für die operative IT-Sicherheit ist die Leitung der Campus-IT. Sie ist für den sicheren Betrieb der zentralen IT und die Umsetzung geeigneter Sicherheitsmechanismen verantwortlich. In Zusammenarbeit mit dem 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 Verantwortlichen („IT-Verantwortliche“) verantwortlich.

Die/der ISB wird frühzeitig in alle anstehenden IT-Projekte eingebunden. Für zentrale IT-Projekte stellt dies die Leitung der Campus-IT sicher, für dezentrale Projekte die Verantwortlichen der jeweiligen IT-Systeme. Darüber hinaus werden die Verantwortlichen („IT-Verantwortliche“) für die an der HdM bestehenden 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 mit einbezogen.

6.4 Arbeitskreis Informationssicherheit

Der Arbeitskreis Informationssicherheit agiert als Informationssicherheits-Management-Team und setzt sich aus der/dem ISB als Vorsitzenden, der/dem Datenschutzbeauftragten, ein bzw. eine/n Vertreter*in der jeweiligen Fakultät, die Technische Betriebsleitung, die Leitung der Core-IT, gegebenenfalls weiteren fachkundigen Mitarbeiter*innen aus der Verwaltung zusammen. Werden weitere fachkundigen Mitarbeiter*innen vom bzw. von der Vorsitzenden benannt, so bedarf es der vorherigen Zustimmung des Rektors bzw. der Rektorin. Die Benennung erfolgt für vier Jahre und kann mehrmals wiederholt werden. Der Arbeitskreis Informationssicherheit hält regelmäßige Treffen ab.

Der Arbeitskreis Informationssicherheit plant die notwendigen Tätigkeiten zur Aufrechterhaltung und Verbesserung der Informationssicherheit an der HdM und berät die/den ISB. Weiterhin werden im Arbeitskreis Informationssicherheit Audits geplant und Sicherheitsvorfälle besprochen. Im Arbeitskreis Informationssicherheit werden auch die Dokumente des ISMS laufend überprüft und überarbeitet. Planungen und Änderungen im Anwendungsbereich sind stets im Arbeitskreis Informationssicherheit 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 der/dem 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 unterstützenden 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 der Hochschulleitung 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 Mitarbeitende, Lehrende und Studierende schädigen.

Verstöße gegen diese Leitlinie können deshalb zivilrechtliche, strafrechtliche, bei Beamten disziplinarische und bei Beschäftigten 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 Informationssicherheitsmanagementsystems werden diverse weiterführende Regelungen geschaffen, welche diese Leitlinie weiter konkretisieren und gleichfalls gültig sind.

9 Inkrafttreten

Die Richtlinie tritt zum 1.1.2022 in Kraft.

Stuttgart, den 30. Dezember 2021

Freigegeben durch den Rektor, Prof. Dr. Alexander W. Roos