Hochschule Magdeburg-Stendal

IT-Sicherheitsrichtlinie

2024

Inhaltsverzeichnis

I. Präambel

Um das Ziel „ausreichende und angemessene IT-Sicherheit“ in der Hochschule Magdeburg-Stendal zu erreichen, wurden die Empfehlungen und Vorschläge des Bundesamts für Sicherheit in der Informationstechnik (BSI) zugrunde gelegt und an die Bedürfnisse der Hochschule Magdeburg-Stendal angepasst. Ausgehend von der Annahme, dass Datenschutz und Informationssicherheit einander gleichberechtigt sind und sich wechselseitig ergänzen, sind beide Gesichtspunkte integraler Bestandteil dieser Richtlinie. Damit soll ein systematischer Weg beschritten werden, der zu einem ganzheitlichen Ergebnis führt. Voraussetzung dafür ist die konstruktive Zusammenarbeit aller Beteiligten.

In der IT-Sicherheitsrichtlinie werden wesentliche Aspekte des Datenschutzes berücksichtigt. Allerdings finden hier nicht alle datenschutzrechtlichen Erfordernisse Beachtung, hauptsächlich betrifft dies die umfangreichen Informationspflichten, die bei der Erhebung, Verarbeitung und Speicherung von personenbezogenen Daten beachtet werden müssen.

Die IT-Sicherheitsrichtlinie befasst sich ausschließlich mit Themen der IT-Sicherheit und des Datenschutzes. Darüber hinaus gehende Aspekte sind ggf. in anderen Dokumenten geregelt.

Diese Richtlinie wurde mit der Absicht entwickelt, allen Mitarbeitenden eine Handreichung zu bieten, um notwendige und angemessene Sicherheitsvorkehrungen bei Planung und Betrieb von Informationstechnik auszuwählen und anzuwenden.

II. Kurzbeschreibung

Die IT-Sicherheitsrichtlinie der Hochschule Magdeburg-Stendal ist das zentrale Regelwerk für alle Themenbereiche der IT-Sicherheit und enthält auch Präzisierungen der datenschutzrechtlichen Anforderungen.

Die Richtlinie ist in den Hauptteil und einen Anhang untergliedert. Im Hauptteil werden Begriffsdefinitionen vorgenommen und wesentliche organisatorische Strukturen festgelegt. Er enthält eine Sammlung von technisch-organisatorischen Grundschutzmaßnahmen, die in jedem Fall umgesetzt werden müssen. Weiterhin wird der Umgang mit bzw. die Anwendung dieser Richtlinie erklärt. Der Anhang beschreibt die Dokumentation des IT-Einsatzes und der Datenverarbeitung. Insbesondere wird in diesem Teil die Methode zur Ermittlung des Schutzbedarfes der verarbeiteten Daten und der Risikoanalyse festgelegt.

III. Einleitung

Die Hochschule Magdeburg-Stendal setzt in hohem Maße Informationstechnologie in ihren Kernprozessen ein.
Verbunden mit dem zunehmenden IT-Einsatz an der Hochschule Magdeburg-Stendal steigt auch die Abhängigkeit der Hochschule vom Funktionieren der IT. Der zuverlässige IT-Einsatz ist notwendig auf Grund von

- Eigeninteresse: Sowohl der Institution als auch persönlich der Institutionsmitglieder;

- gesetzlichen Anforderungen: Zum Beispiel Datenschutz, Haushaltsrecht und Steuerrecht, ordnungsgemäße Geschäftsführung;

- vertraglichen Anforderungen: Zum Beispiel von Drittmittelgebern und bei der Nutzung der Dienste des Deutschen Forschungsnetzes (DFN).

Es sind daher Maßnahmen zu treffen, die die Funktionsfähigkeit der Hochschule Magdeburg-Stendal gewährleisten. Die Maßnahmen sollen Schadensereignisse und deren Auswirkungen minimieren, die durch höhere Gewalt, technisches Versagen, vorsätzliche Handlungen, Irrtum, Nachlässigkeit oder Fahrlässigkeit drohen.

Die Beschäftigten der Hochschule werden grundsätzlich als vertrauenswürdig angesehen. Eine anlasslose Überwachung oder auch nur Verfolgung aller Aktivitäten im Netz ist weder notwendig noch wünschenswert. Ein vertrauensvolles und konstruktives Arbeitsklima, in dem Teamgeist und Eigenverantwortung einen hohen Stellenwert besitzen, bildet die beste Grundlage für einen weitestgehend reibungslosen, sicheren und effektiven Gebrauch der Informationstechnik.

Die vorliegende IT-Sicherheitsrichtlinie bezieht sich auf alle Aspekte des IT-Einsatzes und legt fest, welche Schutzmaßnahmen zu treffen sind. Nur bei geordnetem Zusammenwirken von technischen, organisatorischen, personellen und baulichen Maßnahmen kann ein reibungsloser Betrieb gewährleistet werden. Welche Schutzmaßnahmen zu treffen sind, ist in dieser Richtlinie verbindlich beschrieben.

Die Dokumentation des Umgangs mit Informationstechnik ist die Grundlage jeder sicherheits-technischen und datenschutzrechtlichen Betrachtung. Die Dokumentationspflicht wird an der Hochschule durch die Beschreibung von IT-Verfahren erfüllt.

Der für jeden IT-Arbeitsplatz zu erreichende Grundschutz bildet das Fundament der IT-Sicherheit der Hochschule Magdeburg-Stendal. Die hierfür erforderlichen Maßnahmen werden unabhängig von den einzelnen IT-Verfahren beschrieben. Sind höhere Schutzmaßnahmen erforderlich, müssen zusätzliche verfahrensbezogene Maßnahmen erarbeitet und dokumentiert werden.

1) Geltungsbereich

Die in dieser IT-Sicherheitsrichtlinie beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind für alle Mitglieder und Einrichtungen der Hochschule Magdeburg-Stendal verbindlich. Die IT-Sicherheitsrichtlinie gilt darüber hinaus auch für alle externen Nutzenden der IT-Infrastruktur der Hochschule Magdeburg-Stendal.

Die hier festgelegten Regelungen gelten sowohl für den Betrieb als auch bereits für die Planung des Einsatzes von Informationstechnik.

Alle Nutzenden von IT-Ressourcen der Hochschule Magdeburg-Stendal werden über die für sie relevanten Teile der IT-Sicherheitsrichtlinie informiert. Neue Mitarbeiter der Hochschule Magdeburg-Stendal werden beim Eintritt in die Hochschule auf die geltende IT-Sicherheitsrichtlinie hingewiesen. Nicht-Mitglieder, die IT-Ressourcen der Hochschule Magdeburg-Stendal nutzen, werden von der beauftragenden oder einladenden Stelle auf die für sie relevanten Teile der IT-Sicherheitsrichtlinie hingewiesen. Insbesondere ist zu gewährleisten, dass

- für das leitende Personal die allgemeinen Grundsätze und die Organisation der IT-Sicherheit,
- für alle Verfahrensverantwortlichen die verfahrensspezifischen Regelungen,
- für alle übrigen Anwender/innen die Regelungen des IT-Grundschutzes,

als bekannt vorausgesetzt werden können.

2) Leitlinienfunktion für andere Dokumente

Die in dieser Richtlinie enthaltenen Regelungen müssen bei der Ausarbeitung von speziellen IT-Regelwerken, wie Anleitungen, Benutzungsordnungen u. ä. berücksichtigt werden. Insbesondere dürfen Regelungen in anderen Dokumenten den Regeln der IT-Sicherheitsrichtlinie nicht zuwiderlaufen. Bei widersprüchlichen Aussagen zu IT-Sicherheitsthemen gelten stets die in dieser Richtlinie festgelegten Regelungen.

3) Grundbegriffe

Im Folgenden werden die zentralen Begriffe der IT-Sicherheitsrichtlinie der Hochschule Magdeburg-Stendal erläutert.

IT-Verfahren	Die Summe aller IT-Verfahren soll den gesamten IT-Einsatz an der Hochschule beschreiben.
Verfügbarkeit	Das Schutzziel „Verfügbarkeit“ bezieht sich auf Daten bzw. Verfahren und bedeutet, dass sie zeitgerecht zur Verfügung stehen.
Vertraulichkeit	Das Schutzziel „Vertraulichkeit“ ist gewährleistet, wenn nur Personen, die dazu berechtigt sind, von schützenswerten Daten Kenntnis erhalten können.
Integrität	Das Schutzziel „Integrität“ ist gewährleistet, wenn Daten unversehrt und vollständig bleiben.
Transparenz	Das Schutzziel „Transparenz“ ist gewährleistet, wenn die organisatorischen und technischen Maßnahmen zur Datenverarbeitung so dokumentiert sind, dass sie für die jeweils Sachkundigen in zumutbarer Zeit mit zumutbarem Aufwand nachvollziehbar sind.
Authentizität	Das Schutzziel „Authentizität“ bedeutet, dass Daten jederzeit ihrem Ursprung zugeordnet werden können.
Revisionsfähigkeit	Das Schutzziel „Revisionsfähigkeit“ ist gewährleistet, wenn alle Änderungen an Daten nachvollzogen werden können.
Datenvermeidung, Datensparsamkeit und Erforderlichkeit	Personenbezogene Daten dürfen nur erhoben und verarbeitet werden, solange sie für die Erfüllung der Aufgaben erforderlich sind. Werden personenbezogene Daten nicht mehr benötigt, sind sie zu löschen. Es muss stets begründet werden, warum die Daten benötigt werden.
Zweckbindung	Personenbezogene Daten dürfen nur für den Zweck verwendet werden, zu dem sie erhoben wurden. Werden personenbezogene Daten für diesen Zweck nicht mehr benötigt, sind sie zu löschen.
Belastbarkeit	IT muss so ausgelegt sein, dass sie ungewollten oder mutwilligen Störungen bis zu einem gewissen Grad widerstehen kann.
Informationelles Selbstbestimmungsrecht	Betroffene haben das Recht, selbst über die Preisgabe und Verwendung ihrer Daten zu entscheiden.
IT-Grundschutz	Der IT-Grundschutz ist eine Sammlung von Sicherheitsmaßnahmen zum Aufbau und zur Aufrechterhaltung eines angemessenen Basis-Schutzes für IT-Systeme.

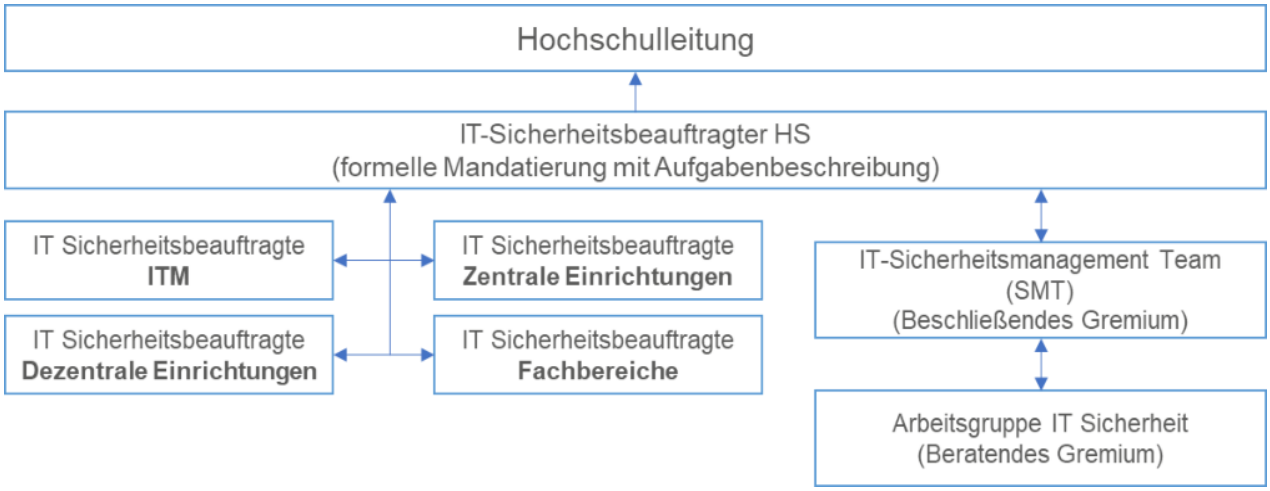
IV. Verantwortlichkeiten

1) Verantwortlichkeiten und Organisation der IT-Sicherheit

Die Vielzahl von IT-gestützten Arbeitsprozessen hat die Verfügbarkeit einer sicheren und zu-verlässigen IT-Infrastruktur zu einem entscheidenden Faktor werden lassen. Der hohe Grad der Vernetzung der Bereiche durch ein übergreifendes Campusnetz kann zur Folge haben, dass sich Sicherheitsmängel in einem Bereich auf die Sicherheit von IT-Systemen in einem anderen Bereich der Hochschule auswirken. Über die Einhaltung der in dieser IT-Sicherheitsrichtlinie aufgestellten Regeln hinaus erfordert die Gewährleistung der IT-Sicherheit die aktive Mitarbeit aller beteiligten Personen, sowohl hierarchie- als auch bereichsübergreifend.

Die an der Hochschule für IT-Sicherheit definierten Rollen und Verantwortlichkeiten werden im Folgenden kurz erläutert:

2) Struktur und Rollen IT-Sicherheit



IT Sicherheitsbeauftragter	Der IT-Sicherheitsbeauftragte ist zuständig für die Koordination und Organisation der IT-Sicherheit innerhalb der Hochschule Magdeburg-Stendal. Er berichtet der Hochschulleitung über relevante, die IT-Sicherheit betreffende Themen und Vorkommnisse sowie regelmäßig den aktuellen Stand der IT-Sicherheit. Er führt Revisionen der IT-Sicherheit durch bzw. veranlasst Revisionen und überprüft damit das aktuelle IT-Sicherheitsniveau. Er übernimmt die Leitung der Analyse und Nachbearbeitung von IT-Sicherheitsvorfällen, die im gemeldet werden. Vorhaben und Änderungen, die die IT-Sicherheit berühren können (z.B. neue IT-Projekte, Änderungen der IT-Infrastruktur, Änderungen von Rahmenbedingungen mit Auswirkungen auf die IT-Sicherheit), müssen mit dem IT-Sicherheitsbeauftragten abgestimmt werden. Die Hochschulleitung setzt zur Unterstützung seiner Arbeit im operativen Bereich die Arbeitsgruppe IT-Sicherheit ein, die vom IT-Sicherheitsbeauftragten der HS geleitet wird. Diese setzt

	sich aus allen dezentralen IT-Sicherheitsbeauftragten zusammen. Die Mitglieder der Arbeitsgruppe IT-Sicherheit repräsentieren die Belange der IT-Sicherheit in den unterschiedlichen Bereichen der Hochschule. Die Arbeitsgruppe IT-Sicherheit berät über alle konzeptionellen und operativen Fragen der IT-Sicherheit und erstellt Empfehlungen für die Hochschulleitung / SMT
Bereichsleitung	Die Leitung eines Bereichs trägt die Verantwortung für den laufenden IT-Einsatz in ihrem Aufgabenbereich sowie für alle bereichsinternen IT-Planungen. Sie benennt einen DV-Organisator, der den IT-Einsatz koordiniert und plant und darüber hinaus die in der IT-Sicherheitsrichtlinie formulierten Maßnahmen umsetzt.
Dezentraler IT-Sicherheitsbeauftragter	Dezentralle IT-Sicherheitsbeauftragte werden vom SMT auf Vorschlag der Leitung eines Bereiches / einer Organisationseinheit ernannt. Jeder Bereich bedarf eines/r IT-Sicherheitsbeauftragten. Diese berichten in sicherheitsrelevanten IT-Themen an den IT-Siciherheitsbeauftragten der HS.
DV-Organisator	Der DV-Organisator bildet die Schnittstelle zwischen der von ihm vertretenden Einrichtung und anderen Bereichen sowie dem ITM. Zum einen bündelt er die Anforderungen und den Bedarf an IT-Unterstützung seiner Einrichtung und kommuniziert diese an das ITM bzw. an die Bereichsleitung (Dekanate, etc.). Zum anderen informiert er die Beschäftigten der Einrichtung über zentrale Vorgaben und sorgt für deren Umsetzung in seinem Bereich.
Verantwortung für den Betrieb eines IT-Verfahrens (Verfahrensverantwortlicher)	Der Verfahrensverantwortliche organisiert die Einführung und den laufenden Betrieb eines IT-Verfahrens einschließlich aller Komponenten und Schnittstellen. Darüber hinaus dokumentiert er das IT-Verfahren. Er ist in der Regel „Besitzer“ der verarbeiteten Daten. Insbesondere trägt er auch die Verantwortung für die Einhaltung des Daten-schutzes und der Informationssicherheit.
Arbeitsgruppe der dezentralen IT-Sicherheitsbeauftragten	Die Arbeitsgruppe der IT-Sicherheitsbeauftragten berät zu allen Fragen der IT-Sicherheit und erstellt Empfehlungen für das SMT der Hochschule Magdeburg-Stendal. Insbesondere entwickelt die Arbeitsgruppe Leitlinien zur IT-Sicherheit, schreibt die zentrale IT-Sicherheitsrichtlinie fort und konzipiert Schulungsprogramme für die IT-Sicherheit. Außerdem unterstützt sie den Informationsaustausch der DV-Organisatoren untereinander und mit dem Servicebereich IT- und Medientechnik (ITM). Durch die Zusammensetzung der Arbeitsgruppe der dezentralen IT-Sicherheitsbeauftragten wird die Vielfalt der unterschiedlichen Anforderungen der Bereiche (Forschung und Lehre, Dienstleister, Verwaltung) an den IT-Einsatz berücksichtigt.
Sicherheitsmanagement-Team (SMT)	i. ein(e) Vertreter(in) der Hochschulleitung, ii. der/die Datenschutzbeauftragte,

	iii. ein(e) Vertreter(in) der dezentralen IT-Sicherheitsbeauftragten, iv. Leiter/-in des ITM, v. Leiter/-in der IuM Kommission.
Höchste Entscheidungsinstanz (Kanzlerin)	Die höchste Entscheidungsinstanz und Träger der Gesamtverantwortung an der Hochschule in allen IT-Fragen ist die Kanzlerin der Hochschule Magdeburg-Stendal. Die hiermit verbundenen Aufgaben können an nachgeordnete Gremien (SMT) und Personen (IT-Sicherheitsbeauftragte) delegiert werden.
IT-Sicherheits-Management-Team (IT-SMT)	Das IT-SMT ist für die Richtlinienerstellung, Fortschreibung, Umsetzung und Überwachung des hochschulweiten IT-Sicherheitsprozesses verantwortlich. Das IT-SMT gibt die hochschulinternen technischen Standards zur IT-Sicherheit vor. Außerdem veranlasst es die Schulung und Weiterbildung der Mitarbeiter auf dem Gebiet der IT-Sicherheit. Das SMT setzt zur Unterstützung seiner Arbeit im operativen Bereich eine Arbeitsgruppe ein. Sie setzt sich aus allen dezentralen IT-Sicherheitsbeauftragten und einem/-r Vertreter/-in des ITM zusammen.
Koordination und Organisation der Informationssicherheit (IT-Sicherheitsbeauftragter der HS)	Die Aufgabe der Koordination und Organisation der Informationssicherheit obliegt dem IT-Sicherheitsbeauftragten der Hochschule Magdeburg-Stendal. Er ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Hochschule.
Datenschutz (Datenschutzbeauftragter)	Dem Datenschutzbeauftragten obliegt die Unterstützung der Hochschulleitung in allen Fragen der Verarbeitung personenbezogener Daten und die Überwachung der ordnungsgemäßen Anwendung datenverarbeitender Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen. Er fungiert als Ansprechpartner für die Angehörigen der Hochschule Magdeburg-Stendal und macht die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Erfordernissen des Datenschutzes vertraut.
Strategische und operative Führung des IT-Einsatzes	Im Auftrag der Hochschulleitung ist der Leiter des Servicebereiches IT- und Medientechnik (ITM) für alle Aufgaben der strategischen Führung der Informationstechnologie und der bereichsübergreifenden operativen Vorgaben verantwortlich.
Bereitstellung von zentralen IT-Diensten	Der Servicebereich IT- und Medientechnik (ITM) plant, realisiert, betreibt und gestaltet IT-Infrastrukturen und -Services für die Einrichtungen der Hochschule Magdeburg-Stendal.

V. Maßnahmen des IT-Grundschutzes

Die in diesem Abschnitt zusammengestellten Maßnahmen bilden die Basis für die IT-Sicherheit an der Hochschule Magdeburg-Stendal. Diese Maßnahmen müssen in jedem Fall umgesetzt werden, soweit sie für das Vorhaben relevant sind.

Für IT-Verfahren mit Schutzbedarf „normal“ ist die Umsetzung der Grundschutzmaßnahmen zum Erreichen eines angemessenen Sicherheitsniveaus ausreichend. Für IT-Verfahren mit hohem oder sehr hohem Schutzbedarf müssen über diese Grundschutzmaßnahmen hinaus zusätzliche Maßnahmen umgesetzt werden. Sie sind verfahrensbezogen und aus der im Anhang beschriebenen Risikoanalyse abgeleitet.

Mit dem Begriff „IT-Personal“ werden im Folgenden alle Personen bezeichnet, die mit der Administration, Wartung und Betreuung von IT-Ressourcen betraut sind. In der Regel handelt es sich um Beschäftigte der Hochschule Magdeburg-Stendal, allerdings wird beispielsweise auch externes Personal dazu gezählt, welches im Rahmen ihrer Beauftragung IT-Ressourcen der Hochschule administriert, wartet oder betreut.

Ausnahmen von den Maßnahmen sollten explizit festgelegt, genehmigt, zeitlich begrenzt und dokumentiert werden. Als Genehmigungsinstanz fungiert der jeweilige IT-Sicherheitsbeauftragte ggf. nach Absprache mit dem IT-Sicherheitsbeauftragten der Hochschule.

1) Allgemeines

(M1) Grundsätze für den IT-Einsatz

Verantwortlich für Umsetzung:	Hochschulleitung

Beschaffung, Entwicklung und Einsatz von IT-Anwendungen und -Systemen, sowie die Verarbeitung von Daten haben sich nach den an der Hochschule Magdeburg-Stendal geltenden Regelungen zu richten.

Die Verantwortung für die Umsetzung und Einhaltung der für den IT-Einsatz geltenden Regelungen tragen die einzelnen Bereichsleitungen in den Fachbereichen, Zentraleinrichtungen und -instituten und der Zentralen Hochschulverwaltung.

(M1a) Schulungsangebot zu IT-Sicherheit und Datenschutz

Verantwortlich für Umsetzung:	Hochschulleitung

Im Rahmen des Weiterbildungsangebots für Beschäftigte der Hochschule Magdeburg-Stendal werden Schulungsangebote zu IT-Sicherheit von der Hochschulleitung auf Vorschlag des SMTs angeboten. Ziel der Schulungsangebote ist es, die Nutzenden der Informationstechnik zu befähigen, spezifische Gefahren zu erkennen und angemessen reagieren zu können.

(M2) Erfassung des IT-Einsatzes

Verantwortlich für Umsetzung:	IT-Beauftragter

Der gesamte IT-Einsatz ist in IT-Verfahren zu gruppieren. Jedes Verfahren ist zu beschreiben. Der/die DV-Organisator/-in informiert die Verfahrensverantwortlichen in seinem/ihrem Zuständigkeitsbereich über ihre Dokumentationspflichten.

(M3) Rollentrennung

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

Für alle IT-Tätigkeiten sind die Verantwortlichkeiten eindeutig festzulegen. Jedem Mitarbeiter und jeder Mitarbeiterin müssen die ihm/ihr übertragenen Verantwortlichkeiten und die ihn/ihr betreffenden Regelungen bekannt sein. Abgrenzungen und Überschneidungen der verschiedenen

Anwenderrollen müssen klar definiert sein. Bei der Rollenbesetzung muss beachtet werden, dass bestimmte Rollen von verschiedenen Personen wahrgenommen werden müssen. Beispielsweise in einem Finanzsystem dürfen die Rollen „sachliche Freigabe“ und „Anordnungsbefugnis“ (Kontrollfunktion vor der Auszahlung) nicht von ein und derselben Person wahrgenommen werden.

(M4) Benennung einer/eines dezentralen IT-Sicherheitsbeauftragten (IT-SiBe)

Verantwortlich für Umsetzung:	Bereichsleitung

Jeder Bereich muss eine/n dezentralen IT-SiBe und eine Abwesenheitsvertretung benennen. Dezentralen IT-SiBe kommt im Rahmen des IT-Einsatzes an der Hochschule eine zentrale Bedeutung zu, denn sie initiieren und koordinieren die Erfassung und Dokumentation des IT-Einsatzes in ihrem Zuständigkeitsbereich. Darüber hinaus bündeln sie die Anforderungen und den Bedarf an IT-Unterstützung ihrer Einrichtung und kommunizieren diese an den IT-Servicebereich der Hochschule bzw. an die Hochschulleitung. Außerdem informieren sie die Beschäftigten der Einrichtung über zentrale Vorgaben und sorgen für deren Umsetzung in ihrer Einrichtung.

(M5) Einbindung der dezentralen IT-SiBe in Entscheidungsprozesse

Verantwortlich für Umsetzung:	Bereichsleitung

Damit die/der dezentralen IT-SiBe ihre/seine Aufgaben effizient wahrnehmen kann, sollte die Stelle des dezentralen IT-SiBe organisatorisch der Bereichsleitung direkt unterstellt sein.
Sie/Er ist in alle Entscheidungsfindungsprozesse mit IT-Relevanz einzubeziehen. Insbesondere muss die/der dezentralen IT-SiBe bei allen IT-Beschaffungsmaßnahmen werden. Darüber hinaus muss die Bereichsleitung sicherstellen, dass die/der dezentralen IT-SiBe über alle IT-relevanten Vorhaben und Planungen des Bereichs frühzeitig Kenntnis erhält.

(M6) Dokumentation der IT-Verfahren

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

IT-Verfahren sind gemäß den im Anhang formulierten Anforderungen zu dokumentieren. Zukünftig sollen nur dokumentierte Verfahren betrieben werden. Die/Der dezentrale IT-SiBe initiiert und koordiniert die Erstellung und Aktualisierung der Dokumentation der Verfahren ihres/seines Bereichs. Die Verfahrensverantwortlichen sind für die Erstellung und Pflege der Dokumentation ihrer Verfahren verantwortlich. Systemadministratoren und Applikations-betreuer sind dabei durch die IT-Sicherheitsordnung zur Mitarbeit verpflichtet.

(M14) Vertretung

Verantwortlich für Umsetzung:	Bereichsleitung

Für alle Betreuungs- und Administrationsfunktionen sind Vertretungsregelungen erforderlich. Die Vertreter müssen alle notwendigen Tätigkeiten ausreichend beherrschen und ggf. auf schriftliche Arbeitsanweisungen und Dokumentationen zurückgreifen können. Die Vertretungsregelung muss organisatorisch festgelegt und nach Möglichkeit auch technisch eingerichtet sein. Dabei muss sichergestellt sein, dass alle Aktivitäten auf eine konkrete Person zurückführbar sind. Beispielsweise sollten anstelle eines generischen Administrator-Accounts einzelne, personenbezogene Accounts mit den erforderlichen Berechtigungen vergeben werden. Die technischen Voraussetzungen für die Wahrnehmung einer Vertretung sollten möglichst ständig eingerichtet sein.

(M15) Qualifizierung

Verantwortlich für Umsetzung:	Bereichsleitung

IT-Personal sollte erst nach ausreichender Schulung mit IT-Verfahren arbeiten. Dabei sind die geltenden Sicherheitsmaßnahmen, die rechtlichen Rahmenbedingungen sowie ggf. die Erfordernisse des Datenschutzes zu erläutern. Es muss sichergestellt sein, dass das IT-Personal in seinen Aufgabengebieten regelmäßig weitergebildet wird.

2) Zugriffskontrolle und Benutzerauthentifizierung

Grundsätzlich gilt, dass nur berechtigte Personen Zugang zu dem Netz und den damit verfügbaren Ressourcen der Hochschule Magdeburg-Stendal erhalten. Jede Nutzungserlaubnis muss personengebunden sein. Die Verwendung fremder Nutzerkennungen, also anderer als der eigenen, ist nicht erlaubt.

a. Benutzerkonten

(M40) Einrichtung anonymer Benutzerkonten

Verantwortlich für Umsetzung:	IT-Personal

Anonyme Benutzerkonten sollten nur in begründeten Ausnahmefällen erlaubt werden. Wenn anonyme Benutzerkennungen eingesetzt werden, müssen geeignete organisatorische Maßnahmen sicherstellen, dass stets nachvollziehbar ist, wer wann wie lange die anonyme Kennung benutzt hat.

(M41) Bereitstellung von Verschlüsselungssystemen

Verantwortlich für Umsetzung:	ITM

Zur Absicherung besonders schützenswerter Daten, insbesondere auf mobilen Geräten, müssen geeignete Systeme (Programme oder spezielle Hardware) zur Verschlüsselung durch die ITM der Hochschule Magdeburg-Stendal bereitgestellt werden.

(M42) Netzzugänge

Verantwortlich für Umsetzung:	DV-Organisatoren, Bereichsleitung

Der Anschluss von Systemen über die Netzzugänge der Hochschule Magdeburg-Stendal hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen in fremde Netze ist unzulässig.

(M43) Ausscheiden oder Wechsel von Mitarbeitern/innen

Verantwortlich für Umsetzung:	Vorgesetzte/r des Mitarbeiters

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass der/die zuständige DV-Organisator/-in rechtzeitig über das Ausscheiden oder den Wechsel einer Mitarbeiterin oder eines Mitarbeiters informiert wird. Vor dem Ausscheiden sind sämtliche Unterlagen und Daten sowie ausgehändigte Schlüssel zurückzugeben. Es sind sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen. Für eine begrenzte Übergangszeit können die Zugangs- und

Zugriffsrechte zur Abwicklung eines geordneten Abschlusses bestehen bleiben. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt, so ist nach dem Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.

(M44) Personenbezogene Kennungen

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r, Anwender

Alle IT-Systeme und Anwendungen sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist eine Anmeldung mit Benutzerkennung und Passwort oder adäquater Verfahren erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel personenbezogen erfolgen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Zugangsdaten weiterzugeben.
Die Einrichtung und Freigabe einer Benutzerkennung dürfen nur in einem geregelten Verfahren erfolgen. Die Einrichtung, Freigabe und Sperrung sind zu dokumentieren.

(M45) Administratorkennungen

Verantwortlich für Umsetzung:	IT-Personal

Das Verwenden von Benutzerkennungen mit Administrationsrechten muss auf die dafür notwendigen Aufgaben beschränkt bleiben. Die Administratoren erhalten für diese Aufgaben eine persönliche Administratorkennung. Für Arbeiten, die keine besonderen Berechtigungsprivilegien erfordern, sind Benutzerkennungen mit eingeschränkten Rechten zu verwenden.

b. Passwörter

(M46) Passwörter

Verantwortlich für Umsetzung:	IT-Personal, Anwender

Werden in einem IT-System Passwörter zur Authentifizierung verwendet, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass mit dem Passwort korrekt umgegangen wird. Die/der Benutzer/-in hat ihr/sein Passwort geheim zu halten. Insbesondere darf das Passwort weder dem IT-Personal noch externen Dienstleistern bekannt gegeben werden.

(M46a) Bildung von Passwörtern

Verantwortlich für Umsetzung:	Anwender

1. Das Passwort darf nicht leicht zu erraten sein, wie zum Beispiel Benutzername, Vor- oder Nachname, Kfz-Kennzeichen, Geburtsdatum. Trivialpasswörter (z.B. "qwertz123" oder "12345678") sind nicht erlaubt.
2. Das Passwort darf nicht aus Wörtern bestehen, die in Wörterbüchern (Passwörterlisten als Grundlage so genannter Wörterbuchangriffe) enthalten sind. z.B. „Hochschule“ oder „Passwort“ als Kennwort.
   Ausnahme: Besteht das Passwort aus mindestens 5 Worten, dann darf das Passwort auch aus Wörtern bestehen, die in einem Wörterbuch enthalten sind.
3. Das Passwort muss mindestens 8 Zeichen lang sein und mindestens eine Ziffer und ein Sonderzeichen enthalten.

(M46b) Umgang mit Passwörtern

Verantwortlich für Umsetzung:	Anwender

1. Voreingestellte Passwörter (z. B. Standardpasswörter des Herstellers bei Auslieferung von Systemen oder Initialpasswörter) müssen durch individuelle Passwörter ersetzt werden.
2. Das Passwort muss geheim gehalten werden und darf bei persönlichen Benutzerkennungen nur der/dem Inhaber/-in der Benutzerkennung selbst bekannt sein.
3. Passwörter, die für Systeme und Dienste der Hochschule Magdeburg-Stendal benutzt werden, dürfen nicht für andere Zwecke verwendet werden.
4. Ein Passwortwechsel ist sofort durchzuführen, wenn der Verdacht besteht, dass das Passwort anderen Personen bekannt geworden ist oder wenn der Verdacht auf eine Systemkompromittierung besteht. Auch wenn Passwörter versehentlich bei anderen Systemen oder anderen Anbietern von Diensten eingegeben wurden, sollte das Passwort gewechselt werden. Bei der Abgabe von Rechnern oder Speichermedien, auf denen Passwörter abgelegt sind, müssen dann die betreffenden Passwörter gewechselt werden, wenn eine vorherige Löschung der Passwörter nicht gewährleistet werden kann (z.B. bei Abgabe eines Rechners im Reparaturfall).

(M46c) Administration von Passwörtern

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

1. Falls technisch möglich, sollten die Bildungsregeln aus (M46a) erzwungen werden.
2. Jede/r Benutzer/-in muss ihr/sein eigenes Passwort jederzeit ändern können.
3. Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. Initialpasswörter müssen individuell unterschiedlich sein und so gewählt werden, dass sie den hier festgelegten Anforderungen genügen.
4. Bei der Authentifizierung in vernetzten Systemen dürfen Passwörter nicht unverschlüsselt übertragen werden.
5. Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

(M46d) Übergabe von Passwörtern

Verantwortlich für Umsetzung:	IT-Personal

Grundsätzlich müssen Passwörter geheim gehalten werden. In Ausnahmefällen dürfen Passwörter nur über geschützte Kommunikationswege an berechtigte Adressaten übergeben werden. Bei der persönlichen Übergabe eines Passworts ist darauf zu achten, dass Unbefugte keine Kenntnis erlangen.

(M46e) Umgang mit SSH-Keys

Verantwortlich für Umsetzung:	Anwender

Wenn persönliche SSH-Keys zur Authentifizierung genutzt werden, muss der private SSH-Key sicher verwahrt und mit einer hinreichend langen Passphrase geschützt werden.

(M47) Zugriffsrechte (Autorisierung)

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r, IT-Personal, Anwender

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Aufgaben bevollmächtigt wird, IT-Systeme, IT-Anwendungen oder Daten zu nutzen. Jeder darf nur mit den Zugriffsrechten arbeiten, die unmittelbar für die Erledigung seiner Aufgaben vorgesehen sind.

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass das zuständige IT-Personal über die notwendige Änderung der Berechtigungen eines Anwenders, z. B. in Folge von Änderungen seiner Aufgaben, rechtzeitig informiert wird.

(M48) Abmelden und ausschalten

Verantwortlich für Umsetzung:	Anwender, IT-Personal

Bei Verlassen des Raumes ist der Zugriff auf das IT-System durch einen Kennwortschutz zu sperren. Soweit technisch möglich ist ein Arbeitsplatz-Rechner so zu konfigurieren, dass dieser nach längerer Inaktivität automatisch gesperrt wird und nur nach erneuter Eingabe eines Passwortes zu aktivieren ist. Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen.

(M49) Verwendung dienstlicher E-Mail-Adressen

Verantwortlich für Umsetzung:	Anwender, IT-Personal

Für dienstliche Belange muss die dienstliche E-Mail-Adresse der Hochschule Magdeburg-Stendal zur elektronischen Kommunikation genutzt werden, sowohl als Empfangs- als auch als Absender-Adresse. Die automatische Weiterleitung der auf der dienstlichen E-Mail-Adresse eingehenden E-Mails auf Mail-Systeme, die nicht von der Hochschule Magdeburg-Stendal betrieben werden, ist nicht zulässig.

(M50) Fernwartung

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r, IT-Personal, Anwender

Bei einer Vereinbarung zur Fernwartung müssen neben den datenschutzrechtlichen Erfordernissen auch die Vorgaben der Hochschule Magdeburg-Stendal beachtet werden.

3) Datenschutz und Datensicherheit

a. Datenschutz

(M8) Regelungen der Datenverarbeitung im Auftrag

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

Eine Datenverarbeitung im Auftrag (ADV) bedarf einer schriftlichen Vereinbarung. Der ADV ist Voraussetzung für alle im Auftrag der Hochschule Magdeburg-Stendal bzw. der/des zuständigen Verfahrensverantwortlichen betriebenen IT-Verfahren. Es sind eindeutige Zuweisungen der Verantwortlichkeit für die IT-Sicherheit zu schaffen und entsprechende Kontrollmöglichkeiten vorzusehen.

Sofern personenbezogene Daten im Auftrag der/des Verfahrensverantwortlichen verarbeitet werden, sind die entsprechenden Regelungen der DSGVO sowie LDS SA anzuwenden.

(M9) Standards für technische Ausstattung

Verantwortlich für Umsetzung:	Zentrale IT-Dienstleister

Um ein ausreichendes Sicherheitsniveau für IT-Systeme zu erreichen, sind Qualitätsstandards im Sinne dieser Richtlinie von den zentralen Dienstleistern unter Maßgabe der vom Rektoratsbeauftragten Digitalisierung (RB Digitalisierung) definierten Strategien zu formulieren und regelmäßig neuen Anforderungen anzupassen. Bei der Entwicklung der Standards sind die spezifischen Bedürfnisse der Fachbereiche zu berücksichtigen.

(M10) Zentralisierung wichtiger Serviceleistungen

Verantwortlich für Umsetzung:	Hochschulleitung, Leitung ITM

Dienste müssen zentral betrieben, angeboten und bei Bedarf genutzt werden, wenn die Zentralisierung deutliche Vorteile mit sich bringt (Kosten, räumliche Sicherheit, Not-stromversorgung, Klimatisierung etc.). An den spezifischen Bedürfnissen eines Fachbereichs ausgerichtete Dienste, deren Betrieb spezielles wissenschaftliches Know-How erfordert, eignen sich hingegen nicht zur Zentralisierung. Dazu gehören beispielsweise IT-gestützte Messanlagen oder spezielle Auswertungs- und Analyse-Informationstechnik.

(M11) Betrieb dezentraler IT-Dienste mit weltweitem Zugriff

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

Grundsätzlich sind Services, die von IT-Dienstleistern der Hochschule Magdeburg-Stendal bereitgestellt werden, selbst betriebenen Diensten vorzuziehen. Nur wenn der benötigte Dienst nicht von zentralen Einrichtungen der Hochschule bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, dürfen der Dienst und die notwendigen IT-Systeme selbst eingerichtet und betrieben werden.

Die notwendige netzwerktechnische Freischaltung von IT-Systemen, die von Netzen außerhalb der Hochschule Magdeburg-Stendal erreichbar sein sollen, muss über die/den zu-ständige/n dezentralen IT-SiBe bei der zuständigen Stelle des ITM beantragt werden. Der Antrag muss begründet sein.

b. Protokollierung

Eine angemessene Protokollierung von IT-Aktivitäten und -Ereignissen ist ein wesentlicher Faktor der Betriebssicherheit. Protokolle dienen u.a. dem Erkennen und Beheben von Fehlern. Mit ihrer Hilfe lässt sich feststellen, wer wann welche Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Für die Verarbeitung personenbezogener Daten ist dies gesetzlich vorgeschrieben.

(M51) Protokollierung durch Betriebssysteme

Verantwortlich für Umsetzung:	IT-Personal

Je nach den Möglichkeiten des Betriebssystems sind alle Zugangsversuche automatisch zu protokollieren. Das Ändern wichtiger Systemparameter sowie das Herunterfahren bzw. das Hochfahren des Systems sollten ebenfalls protokolliert werden.

Bei Servern sind die Protokolle regelmäßig und im Bedarfsfall zeitnah auszuwerten. Es muss dabei sichergestellt sein, dass nur die Personen Zugriff auf die Protokolle erlangen können, bei denen die Protokollauswertung Bestandteil der dienstlichen Aufgaben ist. Das Prinzip der Zweckbindung gemäß der DSGVO und des Landesdatenschutz LSA muss beachtet werden.

(M52) Protokollierung von Netzaktivitäten

Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister

Alle Aktivitäten, die dem Erkennen von Angriffen und Schwachstellen sowie der Überwachung der Betriebssicherheit dienen können, sind für eine spätere Auswertung zu protokollieren. Die Protokolle müssen mit geeigneten Hilfsmitteln regelmäßig ausgewertet werden. Für den Zugriff auf und Umgang mit Protokolldaten und -auswertungen gelten die gleichen Restriktionen wie in (M51).

(M53) Protokollierung durch Anwendungsprogramme

Verantwortlich für Umsetzung:	IT-Personal

Bei der Protokollierung durch Anwendungsprogramme ist der Grundsatz der Datenvermeidung zu beachten, insbesondere sind so wenig personenbezogene Daten wie möglich zu protokollieren. Die erzeugten Protokolldaten sind vor dem Zugriff Unbefugter zu schützen. Die oben genannten Regeln (M61) gelten entsprechend, insbesondere ist bei Daten mit Personenbezug das Zweckbindungsgebot gemäß der DSGVO und des Landesdatenschutz LSA zu beachten.

c. Datensicherung

(M59) Durchführung von Datensicherungen

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

Datensicherungen sollen nach dokumentierten Datensicherungskonzepten erfolgen, welche dem Schutzbedarf der zu sichernden Daten angemessen sind. Im Falle personenbezogener Daten sind die geforderten Mindest- bzw. Höchstzeiträume für die Aufbewahrung der Daten zu beachten.

Das Datensicherungskonzept umfasst alle Regelungen der Datensicherung (was wird von wem nach welcher Methode, wann, wie oft und wo gesichert). Ebenso ist die Aufbewahrung der Sicherungsmedien zu regeln. Alle Sicherungen und das Aufbewahren von Sicherungsmedien – falls vorhanden – sind zu dokumentieren (Datum, Art der Durchführung der Sicherung/gewählte Parameter, Beschriftung der Datenträger, Ort der Aufbewahrung).

(M60) Durchführung der Datensicherung auf Arbeitsplatz-Rechnern

Verantwortlich für Umsetzung:	IT-Personal, Anwender

Grundsätzlich sollten Daten auf zentralen Fileservern gespeichert werden. Dort erfolgt turnusmäßig eine zentrale Datensicherung. Wo ein Zugriff auf einen Fileserver nicht möglich ist, müssen geeignete Maßnahmen zur Datensicherung selbst ergriffen werden.

(M61) Sicherung von Server-Daten

Verantwortlich für Umsetzung:	IT-Personal

Die Sicherung von Server-Daten sollte in angemessenen Intervallen erfolgen. Auch System- und Programmdaten sind nach Veränderungen zu sichern. Zur Datensicherung sind dafür geeignete Backup-Werkzeuge zu verwenden, die eine Datensicherung nach dem Generationenprinzip unterstützen.

Nach Möglichkeit sind die Konfigurationen aller aktiven Netzkomponenten in eine regelmäßige Datensicherung einzubeziehen.

(M62) Verifizierung der Datensicherung

Verantwortlich für Umsetzung:	IT-Personal

Die Konsistenz der Datensicherungsläufe ist sicherzustellen, d. h. die Lesbarkeit der Datensicherung ist zu überprüfen. Das testweise Wiedereinspielen von Datensicherungen soll im Mindestmaß einmal jährlich erfolgen.

d. Datenträgerkontrolle

(M63) Aufbewahrung von Sicherungsdatenträgern

Verantwortlich für Umsetzung:	IT-Personal

Die Sicherungsdatenträger sind getrennt vom jeweiligen Rechner aufzubewahren. Bei Datenbeständen ab Schutzklasse „hoch“ sind die Datenträger in einem anderen Gebäude, einer anderen Brandschutzzone oder in einem für Datenträger geeigneten feuersicheren Umfeld aufzubewahren.

Bei der Lagerung der Datenträger sind die Angaben der Hersteller, insbesondere zu Temperatur und Luftfeuchtigkeit zu beachten. Bei längerer Lagerung sind Vorkehrungen zu treffen, die eine alterungsbedingte Zerstörung der Datenträger verhindern. In angemessenen Zeitabständen ist ein Umkopieren der Daten auf neuere Datensicherungsträger vorzusehen. Die Fortentwicklung der Sicherungssysteme ist zu beachten. Bei einer Langzeitarchivierung muss ggf. die Bereitstellung eines Lesegeräts (ggf. inklusive entsprechender Systemumgebung) eingeplant werden, das für die verwendeten Datenformate geeignet ist.

(M64) Weitergabe von Datenträgern mit schützenswerten Daten

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r, Anwender

Die Weitergabe von Datenträgern, die schützenswerte Daten enthalten, darf nur an befugte Personen erfolgen. Die Weitergabe solcher Daten auf Datenträgern darf nur gegen Quittung erfolgen.

(M65) Herkunft von Datenträgern und gesicherter Transport

Verantwortlich für Umsetzung:	Anwender

Datenträger müssen aus einer zuverlässigen Quelle stammen. Beispielsweise dürfen gefundene USB-Sticks nicht an Geräte oder Netze der Hochschule angeschlossen werden.

Schützenswerte Daten auf mobilen Datenträgern müssen verschlüsselt sein. Ihre Übermittlung hat über einen sicheren Transportweg zu erfolgen. Während des Transports müssen die Datenträger so verpackt sein, dass ein unbefugtes Öffnen festgestellt werden kann.

(M66) Reparatur von IT mit Speichermedien

Verantwortlich für Umsetzung:	IT-Personal

Im Falle eines Austauschs oder einer Reparatur von Geräten muss darauf geachtet werden, dass schützenswerte Daten vorher zuverlässig verschlüsselt, gelöscht oder die betroffenen Datenträger ausgebaut werden. Ist dies nicht möglich, muss das mit der Reparatur beauftragte Unternehmen auf die erforderlichen Informationssicherheitsmaßnahmen und ggf. auf datenschutzrechtliche Vertraulichkeitsvereinbarungen verpflichtet werden.

(M67) Physisches Löschen und Entsorgung von Datenträgern

Verantwortlich für Umsetzung:	IT-Personal, Anwender

Wenn Datenträger, auf denen schützenswerte Daten gespeichert sind, zur weiteren Verwendung an Dritte gehen, müssen alle Datenträger vor der Weitergabe physisch gelöscht werden. Dabei ist auf den Einsatz sicherer Löschverfahren zu achten.

Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Die Datenlöschung ist zu protokollieren.

Bei der Vergabe dieser Aufgaben an externe Dienstleister sind neben der gebotenen Sorgfalt bei der Auswahl des Auftragnehmers auch die übrigen Bestimmungen über Auftragsdatenverarbeitung zu beachten.

4) Netzwerksicherheit

a. Sicherung der Infrastruktur

(M16) Zugang zu Räumen mit zentraler Netzinfrastruktur

Verantwortlich für Umsetzung:	ITM, Facility Management

Die vollständige Zugangskontrolle zu allen Räumen, in denen Geräte mit zentraler Bedeutung für die Netzinfrastruktur der Hochschule Magdeburg-Stendal aufgestellt sind, liegt bei der dafür zuständigen Stelle des ITM. Im Falle einer parallelen Nutzung – soweit dies mit einem sicheren Betrieb der Netzinfrastruktur vereinbar ist – entscheidet die zuständige Stelle des ITM über die Schlüsselvergabe.

(M17) Sicherung der Serverräume

Verantwortlich für Umsetzung:	ITM, Facility Management

Alle Rechnersysteme mit typischer Serverfunktion sind in separaten, besonders gesicherten Räumen aufzustellen. Der Zugang Unbefugter zu diesen Räumen muss zuverlässig verhindert werden. Je nach der Schutzbedürftigkeit sowie in Abhängigkeit von äußeren Bedingungen (öffentlich zugänglicher Bereich, Lage zur Straße usw.) sind besondere bauliche Maßnahmen, wie zum Beispiel einbruchsichere Fenster, einbruchshemmende Türen, Bewegungsmelder o. ä. zur Verhinderung eines gewaltsamen Eindringens vorzusehen.

Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen. Der Zutritt muss auf diejenigen Personen begrenzt werden, deren Arbeitsaufgaben dieses

erfordern. Das Betreten der Räume darf nur nach vorheriger Anmeldung bei der für die Räume verantwortlichen Stelle erfolgen. Fremdpersonal soll sich in Serverräumen nach Möglichkeit nur unter Aufsicht aufhalten.

(M18) Geschützte Aufstellung von Endgeräten

Verantwortlich für Umsetzung:	IT-Personal, Anwender

Der unbefugte Zugang zu Geräten und die unbefugte Benutzung der IT muss verhindert werden. Bei der Anordnung der Geräte ist darauf zu achten, dass Daten mit internem oder vertraulichem Inhalt nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

(M19) Sicherung der Netzknoten

Verantwortlich für Umsetzung:	ITM

Vernetzungsinfrastruktur ist grundsätzlich in verschlossenen Räumen oder in nicht öffentlich zugänglichen Bereichen in verschlossenen Schränken einzurichten, die gegen unbefugten Zutritt und Zerstörung ausreichend gesichert sind. Es gelten die gleichen Empfehlungen wie unter M17.

(M20) Verkabelung und Funknetze

Verantwortlich für Umsetzung:	ITM

Die zentrale Verkabelung des LAN ist nach aktuellen Standards zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Netzwerkadministratoren müssen einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung der Netzkomponenten haben. Für alle Anschlüsse muss durch geeignete Maßnahmen sichergestellt werden, dass nur autorisierte Geräte bzw. Personen einen Netzzugang erhalten. Erweiterungen und Veränderungen an der Gebäudeverkabelung sind mit dem ITM abzustimmen. Funknetze, die mit der IT-Infrastruktur der Hochschule verbunden sind, dürfen nur nach vorheriger Abstimmung mit dem ITM betrieben werden.

(M21) Einweisung und Beaufsichtigung von Fremdpersonal

Verantwortlich für Umsetzung:	ITM, Facility Management

Fremde Personen, die in gesicherten Räumen mit IT (z. B. Serverräume) Arbeiten auszuführen haben, müssen beaufsichtigt werden. Personen, die nicht unmittelbar zum IT-Bereich zu zählen sind, aber Zugang zu gesicherten IT-Räumen benötigen, müssen über die Notwendigkeit besonderer Vorsicht beim Arbeiten in gesicherten Räumen belehrt werden. Alle Aktionen, die von externen Firmen durchgeführt werden, müssen protokolliert werden.

(M22) Stromversorgung und Überspannungsschutz

Verantwortlich für Umsetzung:	Facility Management

Alle wichtigen IT-Systeme dürfen nur an eine ausreichend dimensionierte und gegen Überspannungen abgesicherte Stromversorgung angeschlossen werden. Eine entsprechende Versorgung ist in Zusammenarbeit mit dem Facility Management herzustellen. Die für den Betrieb von IT notwendigen Unterlagen und Informationen zur elektrischen Versorgung sind der/dem DV-Organisator/-in auf Anfrage zur Verfügung zu stellen. Alle Arbeiten an der Stromversorgung müssen mit der/dem DV-Organisator/-in abgestimmt werden.

(M23) USV

Verantwortlich für Umsetzung:	ITM, Facility Management

Alle IT-Systeme, die wichtige oder unverzichtbare Beiträge zur Aufrechterhaltung eines geordneten Betriebes leisten, sind an eine unterbrechungsfreie Stromversorgung (USV) zur Überbrückung von Spannungsschwankungen anzuschließen. Die Konfiguration der USV und der durch sie geschützten Systeme muss ein rechtzeitiges und kontrolliertes Herunterfahren der Systeme gewährleisten.

(M24) Brandschutz

Verantwortlich für Umsetzung:	Brandschutzbeauftragter, Facility Management

Die Regeln des Brandschutzes sind zu beachten und einzuhalten. Insbesondere gilt dies für Räume mit wichtiger Informationstechnik, wie beispielsweise Serverräume. Diese Räume müssen mit geeigneten automatischen Löschvorrichtungen ausgestattete sein. Papier, leere Verpackungen und andere leicht entflammbare Materialien dürfen in diesen Räumen nicht gelagert werden. Die Türen zu diesen Räumen sollen brandhemmend ausgelegt sein. Außerdem sind geeignete Sensoren und geeignete Handfeuerlöscher vorzusehen. Die Maßnahmen sind mit den örtlichen Brandschutzbeauftragten abzusprechen.

(M25) Schutz vor Wasserschäden

Verantwortlich für Umsetzung:	Facility Management

IT-Systeme, die wichtige oder unverzichtbare Komponenten zur Aufrechterhaltung eines geordneten Betriebes darstellen, sind nicht in direkter Nähe zu oder unter wasserführenden Leitungen aufzustellen. Wasserführende Leitungen sollten grundsätzlich nicht in Räumen verlegt werden oder bereits vorhanden sein, in denen wichtige IT-Geräte aufgestellt sind. Wenn die Gefahr eines Wassereintritts besteht, muss sichergestellt werden, dass dieser frühzeitig erkannt wird und geeignete Maßnahmen zur Gefahrenabwehr ergriffen werden können. Auch bei einem Wassereinbruch muss der weitere Betrieb der IT-Systeme gewährleistet sein. Dies gilt insbesondere dann, wenn die IT-Systeme in Kellerräumen aufgestellt werden. So ist beispielsweise besonders darauf zu achten, dass nicht die tiefste Stelle im Gebäude zur Aufstellung der Geräte genutzt wird.

(M26) Klimatisierung

Verantwortlich für Umsetzung:	Facility Management

Der Einbau von Klimatisierungsanlagen wird erforderlich, wenn der Luft- und Wärmeaustausch von Server- und Rechnerräumen unzureichend ist bzw. hohe Anforderungen an die Be- und Entfeuchtung eines Raums und hinsichtlich der Schwebstoffbelastung gestellt werden. Die Gewährleistung der zulässigen IT-Betriebstemperatur und demzufolge die Sicherstellung des IT-Betriebs steht in engem Zusammenhang mit dem störungsfreien Einsatz von Klimatisierungsgeräten. Daher müssen hoch verfügbare Geräte mit genügend Reserveleistung ausgestattet sein. Durch geeignete technische und organisatorische Maßnahmen ist sicherzustellen, dass eine Abweichung von der Soll-Temperatur rechtzeitig erkannt werden kann.

Die Dimensionierung, der Aufstellungsort und weitere Merkmale der Klimatisierungsanlage sollte auf Grundlage sorgfältiger Analysen (z.B. Wärmelastberechnungen) festgelegt werden. In klimatisierten Räumen, die ständig mit Personal besetzt sind, ist eine Frischluft-Beimischung notwendig.

b. Softwareeinsatz

(M27) Beschaffung

Verantwortlich für Umsetzung:	Bereichsleitung

Der Einsatz von Software, von der anzunehmen oder zu vermuten ist, dass sie die IT-Sicherheit gefährden könnte, ist mit den zuständigen DV-Organisatoren abzustimmen. Die Beschaffung von Software muss den zuständigen DV-Organisatoren angezeigt und vom ITM genehmigt werden.

(M28) Berücksichtigung digitaler Signaturen beim IT-Einsatz

Verantwortlich für Umsetzung:	Bereichsleitung, Verfahrensverantwortliche/r

Bei der Auswahl neu zu beschaffender Software soll darauf geachtet werden, dass der Einsatz digitaler Signaturen (Zertifikat) unterstützt wird, soweit dies für den Einsatzzweck relevant ist.
Bestehende Software, die noch nicht mit digitalen Signaturen umgehen kann, ist zu erweitern oder auszutauschen, soweit es technisch möglich und wirtschaftlich vertretbar ist.

(M29) Kontrollierter Softwareeinsatz

Verantwortlich für Umsetzung:	IT-Personal, Anwender

Auf sicherheitsrelevanten Rechnersystemen der Hochschule Magdeburg-Stendal (z.B. Verwaltung, Service-Center, Sekretariate, ITM, etc.) darf aus Gründen des Schutzes von Daten und Technik nur Software installiert werden, die von der zuständigen Stelle dafür freigegeben wurde. Bei der Freigabe muss darauf geachtet werden, dass die Software aus zuverlässiger Quelle stammt und dass ihr Einsatz notwendig ist. Das eigenmächtige Einspielen von Software auf allen anderen Rechnersystemen sollte erst nach Absprache mit den jeweils zuständigen IT-Verantwortlichen erfolgen.

(M30) Test von Software

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r, IT-Personal

Vor der Anschaffung / dem Einsatz neuer Software oder ggf. neuer Versionen muss die Erfüllung der Anforderungen durch hinreichende Tests (durch den die Software Installierenden) sichergestellt sein.

c. System- und Netzwerkmanagement

Die elektronische Kommunikation der Hochschule wird durch eine Sicherheitsinfrastruktur in angemessener Weise geschützt. Besonderes Augenmerk gilt dabei der Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf.

(M54) Sichere Netzwerkadministration

Verantwortlich für Umsetzung:	IT-Personal, ITM

Es muss geregelt und sichergestellt sein, dass die Administration des lokalen Netzwerks nur von dem dafür vorgesehenen Personal durchgeführt wird. Aktive und passive Netzkomponenten sowie Server sind vor dem Zugriff Unbefugter zu schützen. Bereichsübergreifende Netzwerke dürfen ausschließlich von Mitarbeitern des Hochschulrechenzentrums administriert und kontrolliert werden.

(M55) Netzmonitoring

Verantwortlich für Umsetzung:	IT-Personal, ITM

Es müssen geeignete Maßnahmen getroffen werden, um Angriffe, Überlastungen und Störungen im Netzwerk frühzeitig zu erkennen und zu lokalisieren.

Es muss geregelt und sichergestellt sein, dass auf die für diesen Zweck eingesetzten Werkzeuge nur die dazu befugten Personen zugreifen können. Der Kreis der befugten Personen ist auf das notwendige Maß zu beschränken.

(M56) Verhinderung des unbefugten Netzzugangs

Verantwortlich für Umsetzung:	IT-Personal, ITM

Netzwerkzugänge sind so zu konfigurieren, dass ein unbefugter Zugang zum Netz der Hochschule Magdeburg-Stendal verhindert wird.

(M57) Kommunikation zwischen unterschiedlichen Sicherheitsniveaus

Verantwortlich für Umsetzung:	IT-Personal, ITM

Die gesamte Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf oder mit externen Partnern darf ausschließlich über kontrollierte Kanäle erfolgen, die durch ein spezielles Schutzsystem geführt werden. Die Installation und der Betrieb anderer Kommunikationsverbindungen neben den Netzverbindungen der Hochschule Magdeburg-Stendal sind nicht gestattet. Falls auf Grund besonderer Umstände die Installation anderer Kommunikationswege unumgänglich ist, muss dies zuvor durch den zuständigen DV-Organisator und das ITM genehmigt werden. Jeder Zugriff Externer ist zu protokollieren.

(M58) Rechnernamen

Verantwortlich für Umsetzung:	IT-Personal, ITM

Zur Erleichterung der Notfallvorsorge und der Missbrauchsnachverfolgung sollte jedes Gerät, das mit den Netzen der Hochschule Magdeburg-Stendal verbunden ist, einen DNS-Eintrag (DNS = Domain Name System) der Hochschule Magdeburg-Stendal besitzen

5) Endgerätesicherheit

a. Sicherheitsrichtlinien für Computerarbeitsplätze

(M31) Sicherheit von Betriebssystemen und Anwendungen

Verantwortlich für Umsetzung:	IT-Personal

Sicherheitsrelevante Updates und Patches müssen, soweit möglich, zeitnah eingepflegt werden. Software, insbesondere Betriebssysteme, die vom Anbieter nicht mehr mit aktuellen Sicherheitsupdates versorgt wird, darf nicht weiter eingesetzt werden.

In Ausnahmefällen, in denen eine Umstellung aus technischen Gründen nicht möglich ist (zum Beispiel Messrechner), müssen solche Rechner in isolierte Netzbereiche verlagert werden.

Die vom Hersteller gelieferte Grundeinstellung muss überprüft und ggf. entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Nicht benötigte Schnittstellen und Dienste sind zu deaktivieren.

(M32) Schutz vor Schadprogrammen

Verantwortlich für Umsetzung:	IT-Personal, Anwender

Auf allen Arbeitsplatz-Rechnern ist, soweit möglich, ein aktueller Malware-Scanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Regelmäßig (möglichst automatisiert) sind die Erkennungsmuster zu aktualisieren. Wird auf einem System schädlicher Programmcode entdeckt, muss die zuständige Stelle informiert werden.

(M33) Schutz der Rechner-Konfiguration

Verantwortlich für Umsetzung:	IT-Personal

Die Konfiguration von Rechnern muss durch angemessene und geeignete Maßnahmen geschützt werden. Der Umfang der Schutzmaßnahmen richtet sich nach der Bedeutung des Rechners für den laufenden Betrieb und nach dem Schutzbedarf der dort verarbeiteten Daten.

(M34) Ausfallsicherheit

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

Maßnahmen zur Ausfallsicherheit sind entsprechend der jeweiligen Anforderung an die Verfügbarkeit zu ergreifen. IT-Systeme, die zur Aufrechterhaltung eines geordneten Betriebs notwendig sind, müssen durch Ausweichlösungen (redundante Geräteauslegung oder Übernahme durch gleichartige Geräte mit leicht verminderter Leistung) bzw. Wartungsverträge mit entsprechenden Reaktionszeiten hinreichend verfügbar gehalten werden.

(M35) Datenablage in der Cloud und Sync + Share (Nextcloud)

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r, Anwender

Wenn Daten mit Hilfe von Cloud-Diensten gespeichert bzw. verarbeitet werden, drohen spezielle Gefahren, die sich insbesondere aus der Überlassung der Daten an externe Dienstanbieter und der dynamischen Verteilung der Speicherkapazitäten über verschiedene Standorte ergeben. Die (Nicht-)Zulässigkeit der Speicherung in der Cloud richtet sich nach dem Schutzbedarf der Daten. Weitere Einzelheiten können der „Richtlinie zur Auslagerung von Daten in die Cloud“ und den „Sync+Share (Nextcloud) Sicherheitsempfehlungen“ entnommen werden.

Beide Regelwerke sind auf den Webseiten des ITM zum Thema IT-Sicherheit unter „WICHTIGE REGELUNGEN“ abrufbar.

b. Hardwareeinsatz

(M27) Beschaffung

Verantwortlich für Umsetzung:	Bereichsleitung

Der Einsatz von Hardware ist mit der/dem zuständigen DV-Organisators abzustimmen. Die Beschaffung von Hardware muss dem zuständigen DV-Organisators angezeigt und vom ITM genehmigt werden.

c. Einsatz von mobilen Geräten

Durch den Einsatz mobiler Geräte ergeben sich spezielle Gefährdungen, wie zum Beispiel ein erhöhtes Diebstahlrisiko. Dabei ist es unerheblich, ob die Nutzung der mobilen Geräte tatsächlich mobil oder stationär erfolgt. Allerdings sind nicht alle Schutzmaßnahmen anwendbar, die für stationäre Systeme geeignet sind. Die Maßnahmen dieses Abschnitts gehen auf diese spezifischen Gegebenheiten ein. Grundsätzlich gelten alle Maßnahmen, soweit anwendbar, auch für mobile Geräte.

Bei der Beschreibung und Umsetzung der Maßnahmen spielen die Eigentumsverhältnisse keine Rolle, sofern nichts anderes angegeben wird. Es ist also unerheblich, ob es sich um ein privates oder dienstliches Gerät handelt. Die Maßnahmen gelten immer, wenn Ressourcen (Infrastruktur, IT, Daten usw.) der Hochschule Magdeburg-Stendal in Anspruch genommen werden.

(M36) Zugriffsschutz mobiler Dienst-Geräte

Verantwortlich für Umsetzung:	Anwender

Der Zugriff auf mobile dienstliche Geräte und auf deren Anwendungen muss durch Schutzvorkehrungen wie Passwort, PIN usw. abgesichert werden. Der Zugriffsschutz sollte so eingestellt sein, dass er automatisch nach einer angemessenen Zeit der Nicht-Nutzung aktiv wird. Geräte, deren technische Ausstattung keinen Zugriffsschutz bietet, sollten nur beschafft und eingesetzt werden, wenn keine Alternativen zur Verfügung stehen.

(M37) Verlust eines mobilen Dienst-Geräts

Verantwortlich für Umsetzung:	Anwender

Der Verlust eines mobilen Gerätes, auf dem dienstliche Daten gespeichert sind, muss umgehend dem zuständigen IT-Personal gemeldet werden. Dies gilt auch, wenn es sich um ein privates Gerät handelt. Insbesondere bei Mobiltelefonen müssen Maßnahmen zur Sperrung des Geräts bzw. der SIM-Karte getroffen werden. Weitere Maßnahmen, wie zum Beispiel die Lokalisierung des Geräts, die Datenlöschung usw. sind – soweit möglich – ebenfalls sofort durchzuführen.

(M38) Geregelte Übergabe eines mobilen Dienst-Geräts

Verantwortlich für Umsetzung:	Vorgesetzter, Anwender

Bei der Nutzung von mobilen Dienst-Geräten durch verschiedene Personen muss die Übergabe geregelt stattfinden. Dabei muss mindestens nachvollziehbar sein, welche Person das Gerät zu welchen Zeiten besessen hat.

(M39) Schutz der Daten auf mobilen Geräten

Verantwortlich für Umsetzung:	Anwender

Dokumente und Informationen, deren Schutzbedarf hoch oder sehr hoch ist, müssen auf dem mobilen Gerät verschlüsselt abgelegt sein. Bei Mitnahme der Geräte mit verschlüsselten Daten ins Ausland können je nach Zielland die Einreisebestimmungen relevant sein: Einige Länder untersagen die Einfuhr von verschlüsselten Geräten bzw. Datenträgern. Vor Reiseantritt sollten ggf. zusammen mit dem Hochschulrechenzentrum geeignete Vorkehrungen getroffen werden.

6) Incident Response / Umgang mit Störfällen

(M7) Melden und Dokumentieren von Ereignissen bzw. Fehlern

Verantwortlich für Umsetzung:	Anwender, IT-Personal

Ereignisse, die Indiz für einen Sicherheitsvorfall sein können, müssen an eine der folgenden Stellen gemeldet werden:

- dezentralen IT-SiBe
- IT-SiBe der Hochschule

Je nachdem wo der Vorfall gemeldet wird, erfolgt eine erste Bewertung durch die/den dezentralen IT-SiBe. Hier wird über die weiteren Bearbeitungsschritte und über die Information und Einbeziehung weiterer Stellen entschieden.
Jeder Sicherheitsvorfall muss durch die bearbeitende Stelle an die E-Mail-Adresse it-sicherheit@h2.de gemeldet werden.

Die IT-Anwender sind in geeigneter Weise darauf hinzuweisen, dass mögliche Sicherheitsvorfälle (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle u. ä.) dem zuständigen IT-Personal gemeldet werden müssen.

7) Dokumentation

a. Aktualisierung IT-Sicherheitsrichtlinie

(M12) Überprüfung der Wirksamkeit der IT-Sicherheitsmaßnahmen

Verantwortlich für Umsetzung:	Bereichsleitung, IT-Sicherheitsbeauftragter

Die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit und des Datenschutzes sind regelmäßig und nach jeder Änderung der Sicherheitsstandards zu überprüfen. Zeitgleich mit der Änderung der Maßnahmen muss gegebenenfalls die Dokumentation aktualisiert werden.

(M13) Notfallvorsorge

Verantwortlich für Umsetzung:	Verfahrensverantwortliche/r

Bei der Einführung neuer IT-Verfahren bzw. neuer IT-Arbeitsprozesse werden im Rahmen der Dokumentationspflichten, Analysen zur Ermittlung des Schutzbedarfs und ggf. zur Identifizierung und Begegnung spezifischer Risiken vorgenommen. Basierend auf den Ergebnissen dieser Analysen muss gegebenenfalls ein Notfallplan erstellt werden, in dem festgelegt wird, wie auf Notfallsituationen adäquat reagiert wird. „Notfall“ bezeichnet eine Situation, in der durch eine Betriebsstörung die Sicherheit der IT und der Schutz der Daten nicht mehr gegeben ist und ein verhältnismäßig hoher

Schaden entstehen kann. In einem Notfallplan müssen Regelungen zu Verantwortlichkeiten enthalten sein. Außerdem muss ein Alarmierungsplan erstellt werden, in dem die Meldewege und die Kontaktdaten der beteiligten Stellen und Personen im Notfall beschrieben sind.

b. Inkraftsetzung und Aktualisierung der IT-Sicherheitsrichtlinie

Aufgrund der hohen Eigenständigkeit der einzelnen Bereiche wird die Verantwortung für die Umsetzung der IT-Sicherheitsrichtlinie auf die einzelnen Bereiche der Hochschule übertragen. Wesentliche Impulse zur Unterstützung der Verantwortlichen gehen dabei von den dezentralen IT-Sicherheitsverantwortlichen und den DV-Organisator aus.

Der Senat der Hochschule Magdeburg-Stendal setzt die IT-Sicherheitsrichtlinie in Kraft.

Die IT-Sicherheitsrichtlinie bedarf der regelmäßigen Überprüfung und Überarbeitung. Mit der Pflege und Fortschreibung der IT-Sicherheitsrichtlinie der Hochschule Magdeburg-Stendal ist die *Arbeitsgruppe IT-Sicherheit* beauftragt. Die Gewährleistung der Aktualität wird durch die folgende Vorgehensweise sichergestellt:

1.	Überarbeitung der Richtlinie	Die Arbeitsgruppe überarbeitet die Richtlinie und erstellt einen Entwurf / Änderungsvorschläge
2.	Abstimmung	Der IT-Sicherheitsbeauftragte stimmt den Entwurf mit Leiter ITM, Datenschutzbeauftragten und DV Organisatoren ab
3.	Vorlage SMT	Der IT-Sicherheitsbeauftragte legt dem SMT den abgestimmten Richtlinienentwurf vor
4.	Prüfung und In-Kraft-Setzung	Die Hochschulleitung legt nach Prüfung des Entwurfs diesen dem Senat vor und setzt ihn in Kraft.

c. Umsetzung der IT-Sicherheitsrichtlinie

Ist eine einvernehmliche Lösung bei Differenzen über die Anwendung der IT-Sicherheitsrichtlinie in einem Bereich nicht möglich, kann der IT Sicherheitsbeauftragte der Hochschule über den Dissens informiert werden. Der IT Sicherheitsbeauftragte der Hochschule trifft auf Basis der geltenden Richtlinien zeitnah eine Entscheidung in der strittigen Sache.

Stellt eine Stelle in der Hochschule Magdeburg-Stendal einen Sicherheitsmangel in einem IT-Verfahren fest, der zu gravierenden Schäden führen kann, ist der IT-Sicherheitsbeauftragte der Hochschule darüber zu informieren. Der IT-Sicherheitsbeauftragte versucht kurzfristig im Einvernehmen mit allen Beteiligten eine Lösung für das Sicherheitsproblem zu finden. Falls Einvernehmen nicht hergestellt werden kann, informiert der IT-Sicherheitsbeauftragte das SMT. Das SMT entscheidet über das weitere Vorgehen.

Anhang zur IT-Sicherheitsrichtlinie 2024

Inhalt

1. Dokumentation von IT-Verfahren

Inhalt und Umfang einer IT-Verfahrensdokumentation sind abhängig von der Art der im IT-Verfahren erfassten Geschäftsprozesse, der eingesetzten IT-Systeme und der Art der zu verarbeitenden Daten. Zu den unverzichtbaren Bestandteilen einer IT-Verfahrensdokumentation gehören:

a) Zweck des IT-Verfahrens, Zielsetzung, Begründung, Beschreibung der Arbeitsabläufe und Angaben über die gesetzliche Grundlage

b) Schutzbedarfsanalyse (siehe Abschnitt 2)

c) Risikoanalyse in Abhängigkeit vom Ergebnis der Schutzbedarfsanalyse (siehe Abschnitt 3)

d) Beschreibung des Berechtigungskonzepts und der Rollen

e) Angaben über die Anzahl und Art von technischen Einrichtungen und Geräten (IT-System)

f) Beschreibung der Schnittstellen zu anderen IT-Verfahren, IT-Systemen und sonstigen Diensten

g) Angaben über die an IT-Verfahren beteiligten Einrichtungen und Bereiche

h) Angaben zum Standort von Anlagen und Geräten, die wesentliche Funktionen innerhalb des IT-Verfahrens erfüllen, soweit dies möglich ist. Bei nicht eindeutig lokalisierbaren Anlagen und Geräten, z.B. bei Nutzung von Cloud-Diensten, müssen Angaben zum Dienstanbieter und zur Form der Zusammenarbeit erfolgen.

i) Betriebshandbuch mit allen für den Betrieb notwendigen Angaben über die im IT-Verfahren erfassten Systeme und zum Betreuungskonzept. Insbesondere sind Re-gelungen zum Wiederanlauf von IT-Systemen und zur Wiederherstellung von Daten vorzusehen. Der Ablageort des Betriebshandbuchs muss in der Verfahrensdokumentation angegeben werden.

j) Angaben zur Notfallvorsorge (Notfallplan), die beschreiben, wie in einer Notfallsituation adäquat reagiert werden muss. Insbesondere muss ein Alarmierungsplan er-stellt werden, in dem die Meldewege und die Kontaktdaten der beteiligten Stellen und Personen beschrieben sind, die im Notfall informiert werden müssen. Darüber hinaus sollten Angaben und Regelungen zu Verantwortlichkeiten und Angaben zum Zugriff auf das Betriebshandbuch enthalten sein.

k) Soweit personenbezogene Daten verarbeitet werden, müssen die Anforderungen der geltenden Datenschutzvorschriften beachtet werden. Dazu zählen insbesondere Angaben zu folgenden Sachverhalten:
   - Löschung der Daten
   - Sperrung der Daten (soweit zutreffend)

- Archivierung der Daten (soweit zutreffend) Weitergabe von Daten (soweit zutreffend)
- Art und Weise, wie die betroffenen Personen über die Verarbeitung ihrer Daten informiert werden; einschließlich Informationstext
- Art und Weise, wie ein Auskunftsersuchen einer betroffenen Person bearbeitet wird
- Art und Weise, wie die betroffenen Personen bei der Erhebung ihrer Daten informiert werden; einschließlich Informationstext

Wichtiges Merkmal eines IT-Verfahrens ist der längerfristige Charakter der erfassten IT-gestützten Arbeitsabläufe. Ein IT-Verfahren ist so zu strukturieren, dass es weder zu kleinteilig noch zu umfassend ist. Der Geschäftsprozess bildet bei der Erfassung des IT-Einsatzes die Grundlage und ist als Abfolge von zusammenhängenden IT-gestützten oder IT-unterstützenden Tätigkeiten definiert. Als Anhaltspunkt für eine Zusammenfassung oder eine Trennung können u. a. folgende Kriterien dienen:

Trennkriterien	Zusammenfassungskriterien
unterschiedlicher Schutzbedarf	Zusammenhängende Aufgaben
verschiedene Datenkategorien	Praktikabilität
verschiedene „Datenbesitzer“	Arbeitsersparnis

Tabelle 1: Strukturierungskriterien für IT-Verfahren und Geschäftsprozesse.

Ein IT-Verfahren besteht aus einem oder mehreren Geschäftsprozessen, die ein gemeinsames Ziel verfolgen. Die Differenzierung eines IT-Verfahrens in mehrere Geschäftsprozesse ermöglicht, dass auch relativ komplexe IT-Verfahren angemessen behandelt und beschrieben werden können. Idealerweise sollten Geschäftsprozesse so abgegrenzt sein, dass andere IT-Verfahren darauf Bezug nehmen können.

Beispiel für ein IT-Verfahren mit nur einem Geschäftsprozess: **Betrieb eines PC-Pools** Der Betrieb eines PC-Pools beinhaltet typischerweise nur einige wenige Tätigkeiten, die alle der Bereitstellung von Computerarbeitsplätzen dienen.

Beispiel für ein IT-Verfahren mit mehreren Geschäftsprozessen: **Campus Management**

Das Campus-Management-System umfasst eine Vielzahl von zusammenhängen-den Prozessen der Hochschule. Unterschiedlicher Schutzbedarf der Daten, verschiedene Datengruppen sowie verschiedene Dateneigentümer legen eine Differenzierung in mehrere Geschäftsprozesse nahe.

1.1. IT-Verfahrensdatenbank

Für die Dokumentation von IT-Verfahren muss die von der Hochschule zentral bereitgestellte IT-Verfahrensdatenbank genutzt werden. Wesentliche Änderungen eines IT-Verfahrens sind spätestens nach drei Monaten in die Datenbank einzupflegen.

Sollte ein IT-Verfahren unverändert geblieben sein, ist dies jährlich zum Stichtag 31. März auch in der Datenbank zu vermerken. Alle größeren Änderungen an einem IT-Verfahren, die zum Beispiel den Datenschutz berühren oder das Betriebsrisiko verändern, müssen vor der Umsetzung durch eine Änderungsmeldung dem IT-Sicherheitsbeauftragten der Hochschule

Magdeburg-Stendal zur Kenntnis gegeben werden. Dort wird die weitere Vorgehensweise mit der/dem Verfahrensverantwortlichen abgestimmt.

1.2. Struktur der IT-Verfahrensdokumentation

Die Dokumentation eines IT-Verfahrens ist einheitlich strukturiert. Eine Reihe von Komponenten finden sich in nahezu allen IT-Verfahren wieder. Die strukturierte Betrachtung von IT-Verfahren ermöglicht eine ebenso strukturierte Dokumentationsweise, indem die Komponenten der Reihe nach bearbeitet werden. Die folgende Grafik soll die Struktur eines IT-Verfahrens mit den typischen Komponenten veranschaulichen.

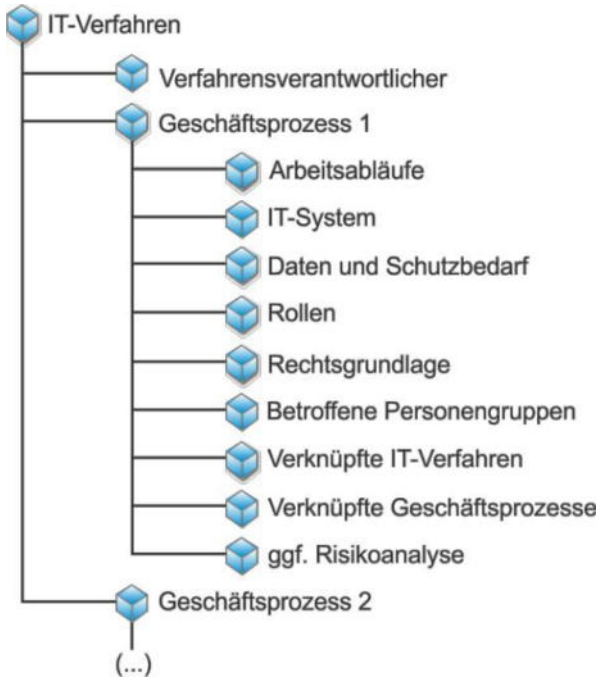


Abbildung 1: Vereinfachte Darstellung der typischen Komponenten eines IT-Verfahrens

1.3. Beziehungen zwischen Komponenten der IT-Verfahrensdokumentation

Die modulare Struktur erlaubt eine Vereinfachung der Verknüpfungsmöglichkeiten durch die Komponenten aus verschiedenen IT-Verfahren. Beispielsweise kann die Nutzung eines vom Hochschulrechenzentrum angebotenen Dienstes dadurch dokumentiert werden, indem auf die Komponente verwiesen wird, die in der Verfahrensdokumentation der ITM den Dienst beschreibt.

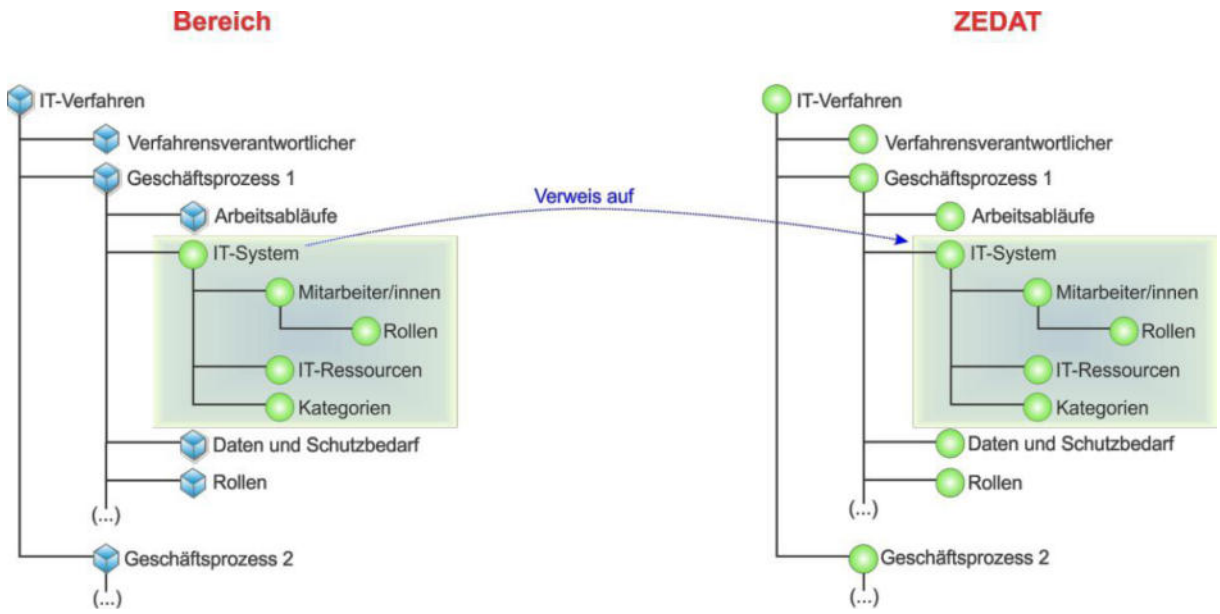


Abbildung 2: Beispiel: Ein IT-Verfahren in einem Fachbereich nutzt einen Dienst des ITM.

1.4. Rollen innerhalb eines IT-Verfahrens

Eine Rolle ist eine Bündelung von Kompetenzen, die zur Bearbeitung von Aufgaben innerhalb eines IT-gestützten Geschäftsprozesses benötigt werden. Sie beschreibt, für welche Aufgaben man mit welchen Rechten auf welche Ressourcen zugreift. Die Rollenverteilung innerhalb eines IT-Verfahrens / Geschäftsprozesses orientiert sich an folgendem Rollenmodell:

Rolle	Funktion	Anmerkung
Verfahrensverantwortlicher	Verantwortlich für • die Einführung und den Betrieb die technische Durchführung bzw. die Erstellung eines Dienstes • die korrekte Umsetzung der für das IT-Verfahren relevanten Vorgaben • alle IT-Aufgaben, die im Rahmen des Verfahrens anfallen • die technische Umsetzung des Datenschutzes und der Informationssicherheit • die Erstellung der Verfahrensdokumentation	• obligatorisch für jedes IT-Verfahren • es kann nur einen Verfahrensverantwortlichen geben • der Verfahrensverantwortliche muss in der Organisationsstruktur so verankert sein, dass er über die notwendigen Befugnisse verfügt
Systemadministrator/in	• installiert, konfiguriert und betreibt IT-Systeme • verantwortlich für den ordnungsgemäßen Betrieb der IT-Systeme	obligatorisch für einen ordnungsgemäßen Betrieb

	• zuständig für die Einhaltung des Betriebs und Datensicherungskonzepts	
Applikationsbetreuer/in	• Parametrisierung und Konfiguration der Anwendungssoftware • Verwaltung von festgelegten Benutzerrechten • administrative Betreuung aus fachlicher Sicht	in der Regel notwendig für einen ordnungsgemäßen Betrieb
Key-User	• Key-User verfügen über besonders gute Anwendungskenntnisse, die sie an die Anwender weitergeben (Multiplikatoren) • erste Ansprechstelle für Anwender	können bei komplexeren Systemen mit vielen Anwendern sinnvoll sein
Anwender/in	• Nutzer des IT-Verfahrens	

Tabelle 2: Rollen innerhalb eines IT-Verfahrens

Die konkrete personelle Zuordnung einer Rolle ist abhängig von dem betreffenden IT-Verfahren. Bei großen und komplexen IT-Verfahren kann eine Rolle auch auf mehrere Personen verteilt sein. Anderseits können bei kleinen IT-Verfahren mehrere Rollen von einer Person wahrgenommen werden. Nicht alle dargestellten Rollen sind in einem konkretem IT-Verfahren zwingend erforderlich. Obligatorisch für jedes IT-Verfahren ist die Rolle des Verfahrensverantwortlichen; sie muss von einer einzigen natürlichen Person wahrgenommen werden.
Das Zusammenwirken der verschiedenen Rollen soll in der folgenden Grafik veranschaulicht werden.

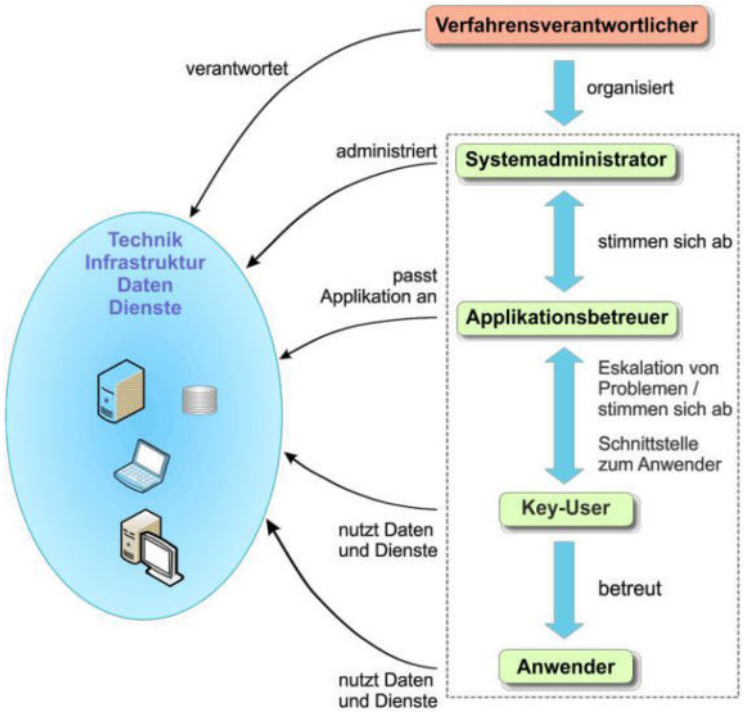


Abbildung 3: Zusammenwirken der Rollen

1.5. IT-Verfahren mit kurzer Betriebsdauer

Für den Betrieb von IT-Systemen in Forschungsprojekten und für IT-Systeme mit kurzer Betriebsdauer (weniger als 12 Monate) entfällt die Pflicht zur ausführlichen Verfahrensbeschreibung, sofern dem keine gesetzlichen Bestimmungen entgegenstehen. (Bei der Verarbeitung personenbezogener Daten müssen beispielsweise die Dokumentationspflichten der Datenschutz-Grundverordnung erfüllt werden.) In jedem Fall ist eine Kurzdokumentation gemäß Abschnitt 2.1 anzulegen und der Betrieb dem IT-Sicherheitsbeauftragten der Hochschule Magdeburg-Stendal anzuzeigen und die Sicherheit der betroffenen Systeme sowie der zugrundeliegenden Infrastruktur zu gewährleisten.

2. Schutzbedarfsanalyse

Die eingesetzte Informationstechnik ist nicht aus sich heraus, sondern vielmehr wegen ihres Wertes für die Anwender schützenswert. Der Wert der Daten und Funktionen, die die IT bereitstellt, ist in der Regel um ein Vielfaches höher als der Wert der Geräte selbst. Daher sind angemessene Sicherheitsmaßnahmen aus den Sicherheitsanforderungen der IT-Verfahren abzuleiten.

Um die Sensibilität der im IT-Verfahren verarbeiteten Daten zu bestimmen, ist die Analyse des Schutzbedarfes durchzuführen. Der Schutzbedarf wird durch die drei Werte (Schutzklassen) „normal“, „hoch“ und „sehr hoch“ klassifiziert. Die im Abschnitt 3.2 wiedergegebenen Tabellen beschreiben die Bedeutung dieser Werte in Hinblick auf verschiedene Kriterien. Aufgrund des Ergebnisses der Schutzbedarfsanalyse können sich darüberhinausgehende Anforderungen ergeben.

Wird als Ergebnis der Schutzbedarfsanalyse das IT-Verfahren in die Schutzklasse „normal“ eingestuft, reichen die Maßnahmen des IT-Grundschutzes im Teil III aus. In allen anderen Fällen muss eine verfahrensspezifische Risikoanalyse durchgeführt werden. Die Vorgehensweise bei einer Risikoanalyse wird im Kapitel 3 beschrieben.

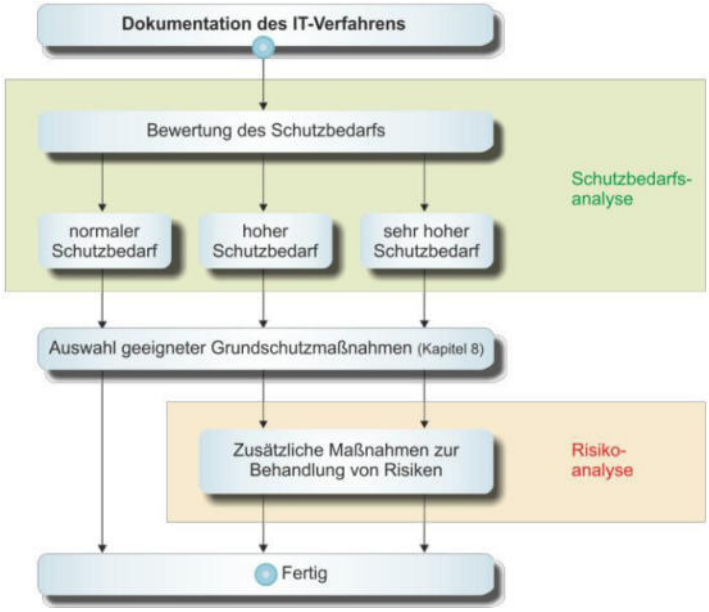


Abbildung 4: Vereinfachte Darstellung der analytischen Schutzbedarfsbewertung

2.1. Vorgehensweise

Die Praxis hat gezeigt, dass die Durchführung der Schutzbedarfsanalyse in einem Team hilfreich ist. Damit mögliche Risiken zuverlässig identifiziert werden, sind detaillierte Kenntnisse über die einzelnen Schritte der Datenverarbeitung notwendig. Häufig sind diese Detailkenntnisse auf mehrere Personen verteilt.

Der Schutzbedarf wird über die Abschätzung der schlimmsten denkbaren Folgen des Verlustes von Vertraulichkeit, Integrität und Verfügbarkeit ermittelt. Die Abschätzung hat gesondert für folgende sechs Schadenskategorien zu erfolgen:

1) Beeinträchtigung des informationellen Selbstbestimmungsrechts
2) Beeinträchtigung der persönlichen Unversehrtheit
3) Beeinträchtigung der Aufgabenerfüllung
4) Negative Außenwirkung
5) Finanzielle Auswirkungen
6) Verstoß gegen Gesetze, Vorschriften und Verträge

Die Durchführung einer Schutzbedarfsanalyse unter Anwendung der unter 2.2 aufgeführten Tabellen wird im Folgenden kurz skizziert. Dabei werden die einzelnen Schritte erläutert und mit Auszügen aus einer fiktiven Beispielanalyse illustriert.

1. Schritt: Identifikation der zu schützenden Daten

An erster Stelle steht die Identifikation aller Daten, die innerhalb des analysierten IT-Verfahrens verarbeitet bzw. gespeichert werden.

Beispiel:
1. Vorname
2. Nachname
3. Straße, Hausnummer

4. Postleitzahl und Ort 5. Forschungsergebnisse 6. Patentanmeldung

2. Schritt: Zusammenfassung der Daten zu Datengruppen (optional)

Häufig lassen sich mehrere Einzeldaten inhaltlich zu Datengruppen zusammenfassen. Die weiteren Schritte sind dann stets auf diese Datengruppen anzuwenden und nicht mehr auf die dort enthaltenen Einzeldaten.
Beispielsweise ist es sinnvoll, Vornamen und Nachnamen sowie die Adressdaten zusammenzufassen. Darum kann eine Datengruppe „Kontaktdaten“ gebildet werden.

Beispiel: 1. Kontaktdaten (Vorname, Nachname, Adresse, Straße, Hausnummer, Postleit-zahl und Ort) 2. Forschungsergebnisse 3. Patentanmeldung

3. Schritt: Bestimmen der schlimmsten möglichen Folgen des Verlustes von Vertraulichkeit / Integrität / Verfügbarkeit (Worst-case-Szenarien)

Jede Datengruppe ist jeweils bezüglich der oben genannten sechs Schadenskategorien zu bewerten. Für jede der sechs Schadenskategorien ist zu überlegen, welche Folgen die Beeinträchtigung der Schutzziele Vertraulichkeit / Integrität / Verfügbarkeit im schlimmsten Fall hätte.

Die Überlegungen sind der Reihe nach bezüglich Verlust der Vertraulichkeit, Integrität und Verfügbarkeit durchzuführen. In jeder der drei Betrachtungen müssen die eingangs genannten Schadenskategorien betrachtet werden.

Beispiele Vertraulichkeit:

Angenommen, Unbefugte erlangen Kenntnis von den Personaldaten: Welche Folgen hätte diese Verletzung des informationellen Selbstbestimmungsrechts im schlimmsten Falle?

→ Der Umgang mit Kollegen und Kolleginnen kann beeinträchtigt werden. Der berufliche Werdegang kann erheblich beeinträchtigt werden.

Angenommen, Unbefugte erlangen Kenntnis von den Personaldaten: Welche Folgen hätte dies im schlimmsten Falle für die persönliche Unversehrtheit?
→ Keine, Folgen für die Gesundheit können ausgeschlossen werden.

(…)

Beispiel Integrität:

Angenommen, Forschungsdaten werden unbefugt verändert: Welche negativen Außenwirkung hätte dies im schlimmsten Falle?

→ Die Hochschule Magdeburg-Stendal würde als unzuverlässige Organisation angesehen werden. Es muss von einem überregionalen Ansehensverlust ausgegangen werden.

(…)

Beispiel Verfügbarkeit:

Angenommen, die Personaldaten stehen nicht zur Verfügung: Welche finanziellen Aus-wirkungen hätte dies im schlimmsten Falle?

→ Es kommt zu Verzögerungen bei der Auszahlung der Bezüge. Die beschäftigten Mitarbeiter/innen müssen mit Abschlagszahlungen rechnen.

(…)

4. Schritt: Einordnung in eine Schutzbedarfskategorie

Die in den Abschätzungsüberlegungen festgestellten schlimmsten Folgen müssen anhand der in den Bewertungstabellen (Abschnitt 2.2) vorgegebenen Maßstäbe (normal / hoch / sehr hoch) eingestuft werden. Das Ergebnis ist zu dokumentieren. Das Maximum des höchsten Schutzbedarfs einer Kategorie bestimmt den Schutzbedarf des IT-Verfahrens. In der folgenden Beispieltabelle würde das gesamte IT-Verfahren in die Schutzklasse „hoch“ eingestuft werden.

Verlust von Vertraulichkeit				
Schadenskategorie	**Bedrohung**	**Abschätzung des Schadens**		
		normal	hoch	sehr hoch
Beeinträchtigung des informationellen Selbstbestimmungsrechts-	Bekannt werden der Daten für Unberechtigte	X		
Beeinträchtigung der persönlichen Unversehrtheit	Missbrauch der Daten ...	X		
Beeinträchtigung der Aufgabenerfüllung	Die Kenntnisnahme der Daten durch Unberechtigte	X		
Negative Außenwirkung	Missbrauch der Daten ...		X	
Finanzielle Auswirkungen	Missbrauch der Daten …	X		
daraus resultierender Schutzbedarf		hoch		

2.2. Bewertungstabellen

Die folgenden vier Bewertungstabellen dienen der Einordnung der Ergebnisse von den Abschätzungsüberlegungen. Die in den Tabellen formulierten Schadensszenarien sollen als Orientierungshilfe genutzt werden. Die Schadensszenarien bezüglich des Verlusts von Vertraulichkeit, Integrität und Verfügbarkeit sowie des Verstoßes gegen Gesetze, Vorschriften und Verträge wurden aus Gründen der besseren Übersicht in vier getrennten Tabellen dargestellt. Demzufolge wiederholen sich zum Teil die skizzierten Szenarien in den Tabellen, aber die Fragestellung ist in jeder Tabelle unterschiedlich.

Mit der Einteilung in drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ folgt diese Richtlinie der Praxis des Bundesamts für Sicherheit in der Informationstechnik (BSI).

2.2.1. Verlust von Vertraulichkeit

Verlust von Vertraulichkeit				
Schadenskategorie	**Schaden**	**Abschätzung des Schadens**		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Missbrauch der Daten kann für die Betroffenen bedeuten:	• Tolerable Beeinträchtigung des informationellen Selbstbestimmungsrechts • Geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse	• Erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts • Erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse	• Gravierende Beeinträchtigung des informationellen Selbstbestimmungsrechts • Gesellschaftlicher oder wirtschaftlicher Ruin
Beeinträchtigung der persönlichen Unversehrtheit	Missbrauch der Daten ...	... führt zu keiner bis leichter Beeinträchtigung der persönlichen Unversehrtheit	... führt zu erheblicher Beeinträchtigung der persönlichen Unversehrtheit	... bedroht die Existenz des Betroffenen
Beeinträchtigung der Aufgabenerfüllung	Missbrauch der Daten würde die Aufgabenerfüllung…	• eines Teilbereichs einer Einrichtung geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. • die Aufgabenerfüllung eines Bereichs ist unwesentlich beeinträchtigt.	• eines Teilbereichs einer Einrichtung erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. • die Aufgabenerfüllung eines Bereichs ist wesentlich beeinträchtigt.	• der gesamten Hochschule gefährden. Kernprozesse der Hochschule können massiv behindert werden.
Negative Außenwirkung	Missbrauch der Daten führt zu ...	• Geringer Ansehensverlust eines Teilbereichs der Hochschule bei einer eingeschränkten Öffentlichkeit	• Ansehensverlust der gesamten Hochschule bei einer eingeschränkten Öffentlichkeit • Hoher Ansehensverlust eines Teilbereichs der Hochschule	Ansehensverlust der gesamten Hochschule in der breiten Öffentlichkeit.
Finanzielle Auswirkungen	Missbrauch der Daten …	Summe der finanziellen Auswirkungen < 150.000 €	Summe der finanziellen Auswirkungen < 3.000.000 €	Summe der finanziellen Auswirkungen >= 3.000.000 €
daraus resultierender Schutzbedarf		**normal**	**hoch**	**sehr hoch**

Tabelle 4: Verlust der Vertraulichkeit

2.2.2. Verletzung von Integrität

Verlust von Integrität				
Schadenskategorie	**Schaden**	**Abschätzung des Schadens**		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Unberechtigte Veränderung der Daten kann für die Betroffenen bedeuten:	• Tolerable Beeinträchtigung des informationellen Selbstbestimmungsrechts • Geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse	• Erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts • Erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse	• Gravierende Beeinträchtigung des informationellen Selbstbestimmungsrechts • Gesellschaftlicher oder wirtschaftlicher Ruin
Beeinträchtigung der persönlichen Unversehrtheit	Unberechtigte Veränderung der Daten	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen Unversehrtheit	... führt zu erheblicher Beeinträchtigung der persönlichen Unversehrtheit	... bedroht die Existenz des Betroffenen
Beeinträchtigung der Aufgabenerfüllung	Unberechtigte Veränderung der Daten würde die Aufgabenerfüllung…	• eines Teilbereichs einer Einrichtung geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. • die Aufgabenerfüllung eines Bereichs ist unwesentlich beeinträchtigt.	• eines Teilbereichs einer Einrichtung erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. • die Aufgabenerfüllung eines Bereichs ist wesentlich beeinträchtigt.	• der gesamten Hochschule gefährden. Kernprozesse der Hochschule können massiv behindert werden.
Negative Außenwirkung	Unberechtigte Veränderung der Daten führt zu:	• Geringer Ansehensverlust eines Teilbereichs der Hochschule bei einer eingeschränkten Öffentlichkeit • Erheblicher Ansehensverlust eines Teilbereichs der Hochschule bei einer sehr kleinen und unbedeutenden Öffentlichkeit	• Ansehensverlust der gesamten Hochschule bei einer eingeschränkten Öffentlichkeit • Hoher Ansehensverlust eines Teilbereichs der Hochschule	Ansehensverlust der gesamten Hochschule in der breiten Öffentlichkeit.
Finanzielle Auswirkungen	Unberechtigte Veränderung der Daten:	Summe der finanziellen Auswirkungen < 150.000 €	Summe der finanziellen Auswirkungen < 3.000.000 €	Summe der finanziellen Auswirkungen >= 3.000.000 €
daraus resultierender Schutzbedarf		**normal**	**hoch**	**sehr hoch**

Tabelle 5: Verletzung der Integrität

2.2.3. Beeinträchtigung von Verfügbarkeit

Mit der Beeinträchtigung der Verfügbarkeit ist sowohl der temporäre als auch der dauerhafte Verlust der Verfügbarkeit gemeint. Allgemein formuliert bedeutet das, dass die Daten bzw. Informationen nicht zur Verfügung stehen, wenn sie gebraucht werden.

Beeinträchtigung der Verfügbarkeit				
Schadenskategorie	**Schaden**	**Abschätzung des Schadens**		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Beeinträchtigung der Daten kann für die Betroffenen bedeuten:	• Tolerable Beeinträchtigung des informationellen Selbstbestimmungsrechts • Geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse	• Erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts • Erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse	• Gravierende Beeinträchtigung des informationellen Selbstbestimmungsrechts • Gesellschaftlicher oder wirtschaftlicher Ruin
Beeinträchtigung der persönlichen Unversehrtheit	Beeinträchtigung der Daten	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen Unversehrtheit	... führt zu erheblicher Beeinträchtigung der persönlichen Unversehrtheit	... bedroht die Existenz des Betroffenen
Beeinträchtigung der Aufgabenerfüllung	Beeinträchtigung der Daten…	• eines Teilbereichs einer Einrichtung geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. • die Aufgabenerfüllung eines Bereichs ist unwesentlich beeinträchtigt.	• eines Teilbereichs einer Einrichtung erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. • die Aufgabenerfüllung eines Bereichs ist wesentlich beeinträchtigt.	• der gesamten Hochschule gefährden. Kernprozesse der Hochschule können massiv behindert werden.
Negative Außenwirkung	Beeinträchtigung der Daten…	• Geringer Ansehensverlust eines Teilbereichs der Hochschule bei einer eingeschränkten Öffentlichkeit • Erheblicher Ansehensverlust eines Teilbereichs der Hochschule bei einer sehr kleinen und unbedeutenden Öffentlichkeit	• Ansehensverlust der gesamten Hochschule bei einer eingeschränkten Öffentlichkeit • Hoher Ansehensverlust eines Teilbereichs der Hochschule	Ansehensverlust der gesamten Hochschule in der breiten Öffentlichkeit.
Finanzielle Auswirkungen	Beeinträchtigung der Daten…	Summe der finanziellen Auswirkungen < 150.000 €	Summe der finanziellen Auswirkungen < 3.000.000 €	Summe der finanziellen Auswirkungen >= 3.000.000 €
daraus resultierender Schutzbedarf		**normal**	**hoch**	**sehr hoch**

Tabelle 6: Beeinträchtigung der Verfügbarkeit

2.2.4. Verstoß gegen Gesetze, Vorschriften und Verträge

Bei der Bearbeitung der Kategorie „Verstoß gegen Gesetze, Vorschriften und Verträge“ müssen alle Regelungen betrachtet werden, die für das betreffende IT-Verfahren relevant sind:

Datenschutzgesetze, beispielsweise
- Landesdatenschutzgesetz Sachsen-Anhalt
- Informationsverarbeitungsgesetz (IVG)
- Bundesdatenschutzgesetz (BDSG)
- Datenschutzgrundverordnung (DSGVO)

Hochschulgesetze bzw. -verordnungen, h2-Richtlinien, beispielsweise
- Hochschulgesetz
- IT-Sicherheitsrichtlinie der Hochschule Magdeburg-Stendal

Vorschriften zur Mitbestimmung, beispielsweise
Landespersonalvertretungsgesetz
IT-Grundsatzdienstvereinbarung der Hochschule Magdeburg-Stendal

Verträge, beispielsweise
Vertrag über die Zusammenarbeit mit einer externen Firma

<table>
<tr><th>Bedrohung</th><th colspan="3">Abschätzung des Schadens</th></tr>
<tr><td></td><td>normal</td><td>hoch</td><td>sehr hoch</td></tr>
<tr><td>Bekannt werden der Daten für Unberechtigte ...</td><td rowspan="3">… verstößt gegen Gesetze oder Vorschriften mit geringen Konsequenzen.[3)]

… hat geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen zur Folge.</td><td rowspan="3">… verstößt gegen Gesetze oder Vorschriften mit erheblichen Konsequenzen.[3)]

… hat Vertragsverletzungen mit hohen Konventionalstrafen und / oder erheblichen Haftungsschäden zur Folge.</td><td rowspan="3">... verstößt gegen Gesetze oder Vorschriften mit schwerwiegenden rechtlichen Konsequenzen.[3)]

… hat Vertragsverletzungen zur Folge, deren Haftungsschäden für die Hochschule sehr hoch sind.</td></tr>
<tr><td>Unberechtigte Veränderung der Daten …</td></tr>
<tr><td>Verlust der Daten</td></tr>
<tr><td>daraus resultierender Schutzbedarf</td><td>normal</td><td>hoch</td><td>sehr hoch</td></tr>
</table>

Tabelle 7: Verstoß gegen Gesetze, Vorschriften und Verträge
Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren:
Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“.

[3)] Zur Einschätzung der rechtlichen Konsequenzen kann das vom Gesetzgeber vorgesehene Strafmaß hilfreich sein.

Die Dokumentation der Schutzbedarfsanalyse besteht aus den Ergebnissen der Bewertungs-tabellen und weiteren Angaben über die analysierten Datensätze bzw. das analysierte IT-Verfahren. Insbesondere müssen die wesentlichen Überlegungen, die zu den einzelnen Einschätzungen über den zu erwartenden Schaden geführt haben, nachvollziehbar dokumentiert werden.

3. Risikoanalyse

Für alle Daten bzw. Datenverarbeitungsschritte, für die in der Schutzbedarfsanalyse ein erhöhter Schutzbedarf ermittelt wurde (Schadensstufe „hoch“ oder „sehr hoch“), muss zusätzlich eine Analyse der Risiken durchgeführt werden. Im Unterschied zur Schutzbedarfsanalyse wer-den in der Risikoanalyse die schadensverursachenden Ereignisse betrachtet.

1. Schutzbedarfsanalyse	Fragestellung:	Welche Schäden können entstehen?
2. Risikoanalyse	Fragestellung:	Welche Ereignisse können Schäden hervorrufen? Welche Eintrittswahrscheinlichkeit besteht für das Ereignis?

Tabelle 8: Unterschied zwischen der Schutzbedarfsanalyse und der Risikoanalyse

Die dabei ermittelten untragbaren Risiken müssen durch geeignete Vorkehrungen und Maßnahmen auf ein tragbares Maß reduziert werden. Diese sind in geeigneter Weise zu dokumentieren. Nach Abschluss der vollständigen Dokumentation bestätigt der/die Verfahrensverantwortliche in Kenntnis der Restrisiken, dass der Betrieb des IT-Verfahrens den für die Hochschule geltenden Sicherheitsanforderungen genügt.

3.1. Begriffsdefinitionen

Der Begriff „Risiko“ ist definiert als Maß der Gefährdung, die von einer Bedrohung ausgeht. Das Risiko setzt sich aus zwei Komponenten zusammen: der Wahrscheinlichkeit, mit der das Ereignis eintritt und der Höhe des Schadens, der als Folge des Ereignisses auftritt.
Für die Abschätzung, mit welcher Wahrscheinlichkeit ein Schaden zu erwarten ist, werden Werte von „selten“ bis „häufig“ verwendet. Dabei werden den Werten die in der folgenden Tabelle aufgeführten Bedeutungen unterlegt.

Häufigkeit	Bedeutung
selten	Das Schadensereignis tritt höchstens alle 5 Jahre ein.
mittel	Das Schadensereignis tritt einmal alle 5 Jahre bis einmal im Jahr ein.
häufig	Das Schadensereignis tritt häufiger als einmal im Jahr ein.

Tabelle 9: Häufigkeitswerte der Eintrittswahrscheinlichkeit von Schäden

Es wird unterschieden zwischen den zwei Risikoklassen „tragbar“ und „untragbar“. Die Zuordnung von Risiken zu einer bestimmten Risikoklasse erfolgt anhand der nachstehenden Tabelle 10. Dabei bedeuten:

Tragbar – akzeptables Risiko
Untragbar – nicht akzeptables Risiko

Schadenshöhe / Häufigkeit	hoch 2	sehr hoch 3
selten	Tragbar	Tragbar
mittel	Tragbar	Untragbar
häufig	Untragbar	Untragbar

Tabelle 10: Risikoklassen

Kategorie	Beispiele
Gebäude	Türen, Brandschutz, Alarmanlage
Räume	Serverraum, Klimaanlage
Hardware	Server, Client
Software	Datenbank, Web-Applikation
Infrastruktur	Kabel, aktive Netzkomponenten, Stromversorgung-
Personen	Administratoren, Nutzer
Kommunikation	E-Mail-Dienst, Telefonie
Datenträger	Papier, USB-Stick

Tabelle 11: Kategorien von Zielobjekten

3.2. Vorgehensweise

Die Risikoanalyse wird in mehreren Schritten durchgeführt. Ausgehend von der Erfassung aller für den Betrieb eines IT-Verfahrens benötigten Zielobjekte werden die folgenden Arbeitsschritte durchgeführt:

Schritt 1	Identifizierung der an dem Geschäftsprozess bzw. das IT-Verfahren beteiligten Komponenten
Schritt 2	Bestimmung der relevanten Komponenten, basierend auf dem Ergebnis der Schutzbedarfsanalyse
Schritt 3	Bestimmung der Gefährdungen je Zielobjekt
Schritt 4	Abschätzung der Häufigkeit von Schäden je Zielobjekt
Schritt 5	Zusammenstellung und Bewertung (Klassifizierung) der Risiken
Schritt 6	Auswahl der Maßnahmen zur Reduzierung der untragbaren Risiken auf ein tragbares Maß
Schritt 7	Erklärung zur Übernahme der Restrisiken durch die/den Verfahrensverantwortliche/n

Untragbare Risiken müssen durch zusätzliche Maßnahmen auf das für die Hochschule Magdeburg-Stendal tragbare Maß reduziert werden. Das Ergebnis der Risikoanalyse beinhaltet nur die zusätzlich notwendigen, über den Grundschutz hinausgehenden Maßnahmen. Der/die Verfahrensverantwortliche hat zu entscheiden, ob durch die umgesetzten Schutzmaßnahmen das Risiko tragbar und somit der Betrieb des IT-Verfahren in der vorgesehenen Form verantwortbar für die Hochschule Magdeburg-Stendal ist.

Bei der Bestimmung der Gefährdungen der ermittelten Zielobjekte (Schritt 3) soll die folgende Tabelle behilflich sein. Sie bietet eine – nicht abschließende – Übersicht über die elementaren Gefährdungen sowie die Nennung der hauptsächlich betroffenen Grundwerte (Vertraulichkeit, Integrität und Verfügbarkeit).

Maßnahmen [4)]	**Gefährdung**	**Vertraulichkeit**	**Integrität**	**Verfügbarkeit**
M28 /M24	Feuer			
M30 / M26	Ungünstige klimatische Bedingungen			
M29 /M25	Wasser			
M19, M20 / M16,M17	Verschmutzung, Staub, Korrosion			
M27 / M23	Ausfall oder Störung der Stromversorgung			
M22, M23, M24 /M19,M20	Ausfall oder Störung von Kommunikationsnetzen			
M41 /M34	Ausfall oder Störung von Dienstleistern			
M25 / M21	Ausspähen von Informationen / Spionage			
M41, M42, M46 / M34 , M37	Verlust von Geräten, Datenträgern und Dokumenten			
?	Fehlplanung oder fehlende Anpassung			
M48, M60 / M39, M49	Offenlegung schützenswerter Informationen			
M35 / M29	Informationen aus unzuverlässiger Quelle			
	Manipulation von Hard- und Software			
	Manipulation von Informationen			
M8 / M7	Unbefugtes Eindringen in IT-Systeme			
M41 / M34	Ausfall von Geräten oder Systemen			
M37 / M31	Fehlfunktion von Geräten oder Systemen			
M16 / M14/,M15	Ressourcenmangel			
M37 /M31	Software-Schwachstellen oder -Fehler			
M3, M7 /M2, M6	Verstoß gegen Gesetze oder Regelungen			
M4, M52, M57/ M3, M43, M47	Unberechtigte Nutzung oder Administration von Geräten und			
M18, M39 / M15, M33	Fehlerhafte Nutzung oder Administration von Geräten und Systemen			
M1a, M4, M52, M54, M56, M57 /M1a, M3,M43, M45, M46,M47	Missbrauch von Berechtigungen			
M16, M17 /M14,M15	Personalausfall			

M53, M56, M59 /M44, M46,M	Identitätsdiebstahl			
	Missbrauch personenbezogener Daten			
M35, M38 / M29,M32	Schadprogramme			
M8, M14, M61, M61a, M62, M64	Störung von Diensten (Denial of Service)			
	Sabotage			
M1a, M80 /M1a,M	Social Engineering			
M19 /M16	Unbefugtes Eindringen in Räumlichkeiten			
M68, M69, M70,/ M59,M60,M61	Datenverlust			
M71, M72/ M62, M63				
	Integritätsverlust schützenswerter Informationen			

3.3. Beispiel

Anhand des folgenden Beispiels soll die Vorgehensweise bei der Risikoanalyse verdeutlicht werden. Das Beispiel-IT-Verfahren besteht nur aus dem Betrieb eines Fileservers. Darum wird nur die Gruppe der Komponenten betrachtet, die für den Betrieb des Fileservers relevant sind. Die grüne unterbrochene Linie soll diese Abgrenzung kennzeichnen.

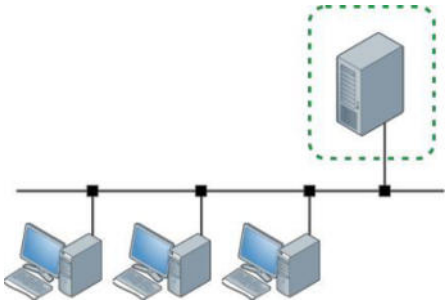


Abbildung 5: Fileserver in einer Netzwerkumgebung.

Ausgangssituation: Die Schutzbedarfsanalyse hat ergeben, dass die auf dem Fileserver ab-gelegten Daten vertraulich behandelt werden müssen (Schutzbedarf „hoch“). Für die Verfügbarkeit und Integrität der Daten wurden keine besonderen Anforderungen ermittelt. Daher muss in diesem Beispiel nur die Vertraulichkeit berücksichtigt werden.

Schritt 1: Identifizierung der an dem IT-Verfahren beteiligten Komponenten.

Nr.	Komponente	Beschreibung
1	Fileserver	Der Fileserver ist ein Stand-alone-System, das unter „Windows Server“ läuft und Netzwerk-Ordner über SMB zur Verfügung stellt
2	Clients	Die Clients werden dezentral administriert oder im Fall von Laptops als „Bring Your Own Device“ (BYOD) eingesetzt
3	Netzwerk	Das Netzwerk wird zentral administriert. Die aktiven und passiven Komponenten sind öffentlich nicht zugänglich. Die Glasfaser- und Kupferleitungen gehören dem Betreiber.
4	Nutzer	Die Nutzung erfolgt durch die Mitarbeiter des Fachbereiches.
5	Administratoren	Die Administration wird durch eine festangestellte Teilzeitkraft so wie studentische Hilfskräfte erledigt.
6	Räume	Der Raum, in dem sich der Server befindet, ist ein Technikraum im Fachbereich, der gleichzeitig auch anderweitig genutzt wird. Der Zugang ist verschlossen, allerdings ist die Verteilung der Schließberechtigung unübersichtlich.
7	Anwendung (Software)	Für die Veröffentlichung der Netzlaufwerke werden die Bordmittel von Windows genutzt.

Schritt 2: Bestimmung der relevanten Komponenten, basierend auf dem Ergebnis der Schutzbedarfsanalyse [5)].

Nr.	Komponente	Relevanz
1	Fileserver	relevant
2	Clients	nicht relevant
3	Netzwerk	relevant
4	Nutzer	nicht relevant
5	Administratoren	relevant
6	Räume	relevant
7	Anwendung (Software)	relevant

Die Relevanz der Komponenten ergibt sich aus der Abgrenzung des betrachteten Bereichs. Für den Betrieb des Fileservers sind der Server selbst und die darauf installierte Software relevant. Außerdem sind das angeschlossene Netzwerk, die für den Betrieb zuständigen Administratoren sowie der Aufstellungsort des Servers relevant. Die Nutzer und die am Netz an-geschlossenen Client-Geräte sind für den Serverbetrieb nicht relevant.

Schritt 3: Bestimmung der Gefährdungen der ermittelten Komponenten.

Nr.	Zielobjekt	Gefährdung
1	Fileserver	unerlaubter Zugriff
3	Netzwerk	abhören
5	Administratoren	ausspähen
6	Räume	unerlaubter Zugriff
7	Anwendung (Software)	unerlaubter Zugang

Schritt 4: Abschätzung der Häufigkeit von Schäden.
Bei der Abschätzung der Häufigkeit von Schäden kann ein Blick in die vergangenen Jahre hilfreich sein. Tritt bei vergleichbaren Szenarien eine Häufung von Schäden bei bestimmten Zielobjekten auf, kann dies ein Hinweis sein. Werden keine Anhaltspunkte gefunden, kann oft eine Befragung der Administratoren oder Anwender in diesem Bereich nützlich sein.

Nr.	Zielobjekt	Gefährdung	Häufigkeit
1	Fileserver	unerlaubter Zugriff	häufig
3	Netzwerk	abhören	selten
5	Administratoren	ausspähen	selten
6	Räume	unerlaubter Zugriff	selten
7	Anwendung (Software)	unerlaubter Zugang	mittel

Schritt 5: Zusammenstellung und Bewertung (Klassifizierung) der Risiken.

Nr.	Zielobjekt	Gefährdung	Häufigkeit	Schadenshöhe	Risiko
1	Fileserver	unerlaubter Zugriff	häufig	hoch	untragbar
3	Netzwerk	abhören	selten	hoch	tragbar
5	Administratoren	ausspähen	selten	hoch	tragbar
6	Räume	unerlaubter Zugriff	selten	hoch	tragbar
7	Anwendung (Software)	unerlaubter Zugang	mittel	hoch	tragbar

Schritt 6: Auswahl der Maßnahmen zur Reduzierung der untragbaren Risiken.
Geeignete Maßnahmen können sowohl technische als auch organisatorische Maßnahmen sein. In diesem Beispiel wäre der Einsatz einer Firewall eine geeignete technische Gegenmaßnahme, um die häufigen Zugriffsversuche auf den Fileserver abzuwehren:

Maßnahme 1:
Installation und Betrieb einer Paketfilter-Firewall, die den gesamten Datenverkehr zum Fileserver kontrolliert. Durch geeignete Filtereinstellungen werden nur die erlaubten Datenpakete weitergeleitet.

Schritt 7: Erklärung zur Übernahme der Restrisiken durch die/den Verfahrensverantwortliche/n:
Der/die Verfahrensverantwortliche bestätigt in Kenntnis der Restrisiken, dass der Betrieb des IT-Verfahrens den für die Hochschule geltenden Sicherheitsanforderungen genügt.

Die Dokumentation der Risikoanalyse besteht im Wesentlichen aus drei Teilen:

1) dem zu betrachtenden Bereich eines IT-Verfahrens (Abgrenzung)
2) den oben skizzierten Tabellen (Dabei ist es nicht nötig, für jeden Schritt eine eigene Tabelle anzulegen. Sinnvoller wäre eine einzige Tabelle, die schrittweise ausgefüllt wird; siehe folgende Tabelle 18.)

3) der Beschreibung der Maßnahmen

Nr.	Zielobjekt	Gefährdung	Häufigkeit	Schadenshöhe	Risiko	Maßnahme
1	Fileserver	unerlaubter Zugriff	häufig	hoch	untragbar	Maßnahme 1
3	Netzwerk	abhören	selten	hoch	tragbar	
5	Administrato-ren	ausspähen	selten	hoch	tragbar	
6	Räume	unerlaubter Zugriff	selten	hoch	tragbar	
7	Anwendung (Software)	unerlaubter Zugang	mittel	hoch	tragbar	

In diesem Bespiel wird bewusst eine sehr einfache IT-Landschaft zugrunde gelegt, damit die Vorgehensweise der Risikoanalyse verdeutlicht werden kann. Aus diesem Grund bleiben auch die Vorteile der modularen Dokumentationsstruktur hier unerwähnt. In einem näher an der Realität orientierten Beispiel hätte das Zielobjekt „Netzwerk“ nach Schritt 2 (Bestimmung der relevanten Komponenten) nicht weiter analysiert werden müssen, denn ein Verweis auf das Dokumentationsmodul „Netzwerk“ des Hochschulrechenzentrums hätte ausgereicht. Der Be-trieb des Netzwerks liegt in der Zuständigkeit des Hochschulrechenzentrums, dort muss es auch vollständig, also inkl. Risikoanalyse, dokumentiert werden.

Bei komplexen IT-Landschaften, d.h. die Liste der relevanten Zielobjekte ist lang, können nach Schritt 2 alle Zielobjekte als erledigt angesehen werden, die an anderer Stelle bereits dokumentiert wurden. Für jedes dieser Zielobjekte muss lediglich auf das betreffende Dokumentationsmodul der anderen Stelle verwiesen werden.