IT-Sicherheitsrichtlinie der Hochschule Magdeburg-Stendal
GRUNDSCHUTZ

Inhalt

1. Vorbemerkung

Um das Ziel „ausreichende und angemessene IT-Sicherheit“ im Bereich der Hochschule Magdeburg-Stendal zu erreichen, wird in Anlehnung an die Empfehlungen und Vorschläge des „Bundesamts für Sicherheit in der Informationstechnik“ (BSI) das folgende Modell des IT-Sicherheitsprozesses zugrunde gelegt. Damit soll ein systematischer Weg beschritten werden, der zu einem ganzheitlichen und vollständigen Ergebnis führt.

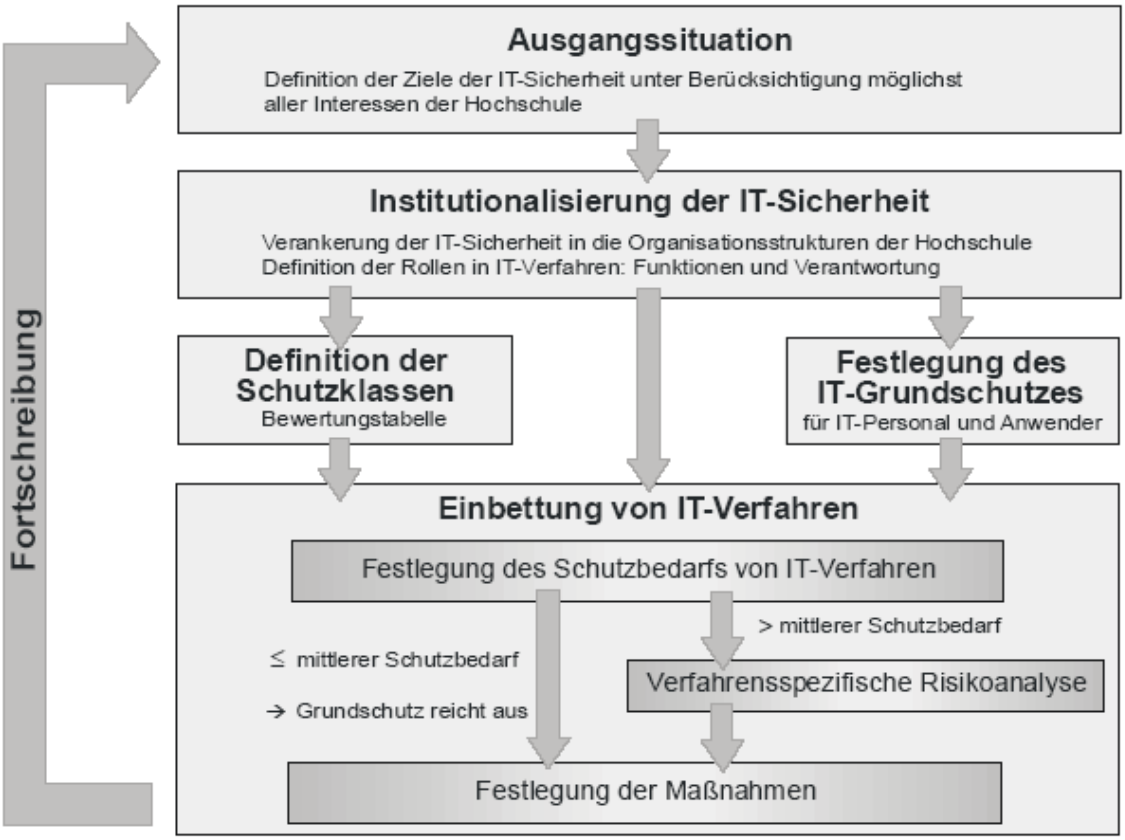

Abbildung 1: Modell des IT-Sicherheitsprozesses, Quelle ZKI e.V,, IT-Sicherheit an Hochschulen

Die Gliederung der vorliegenden Richtlinie orientiert sich an der Abfolge der Schritte im IT-Sicherheitsprozess.. Die in dieser IT-Sicherheitsrichtlinie beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind für die Einrichtungen der Hochschule Magdeburg-Stendal verbindlich.

In diesem Dokument wird die Formulierung „Organisationseinheit“ als Sammelbegriff verwendet und umfasst alle Einrichtungen der Hochschule Magdeburg-Stendal, einschließlich der Fachbereiche, Institute und Zentralen Einrichtungen sowie der Dezernate der Hochschulverwaltung und des Rektorates.

2. Ausgangssituation

Die Hochschule Magdeburg– Stendal setzt in ihren Kernprozessen in hohem Maße IT-Verfahren ein:

- Allgemeine Kommunikation: E-Mail, WWW
- Lehre: zum Beispiel e-Learning, das Bibliothekssystem mit seinen Subsystemen (Datenbankrecherche, Elektronische Zeitschriftenbibliothek)
- Verwaltung: zum Beispiel HIS, Verwaltung von Personaldaten, Finanzsteuerung, Online-Studierendenservice
- Forschung: zum Beispiel weltweite Kommunikation und Zusammenarbeit, elektronische Publikation und Recherche, rechenintensive Anwendungen, IT-gestützte Messverfahren mit hohem Datenaufkommen

Verbunden mit dem steigenden IT-Einsatz an der Hochschule steigt auch die Abhängigkeit der Hochschule vom Funktionieren der IT. Der zuverlässige IT-Einsatz ist notwendig auf Grund von gesetzlichen Anforderungen: zum Beispiel Datenschutz, Haushalts- und Steuerrecht oder auch resultierend aus Prüfungsordnungen. IT-Sicherheit ist ebenso wesentlich zur Sicherung der Lehre und um Imageschaden für die Hochschule zu vermeiden.

Es sind daher Maßnahmen zu treffen, die die Funktionsfähigkeit der Hochschule Magdeburg-Stendal gewährleisten und die Verfügbarkeit, Vertraulichkeit und Integrität der Daten sicherstellen. Die Maßnahmen sollen Schadensereignisse abwehren und so Schäden vermeiden, die durch höhere Gewalt, technisches Versagen, Nachlässigkeit oder Fahrlässigkeit drohen.

Die Mitarbeiter und Mitarbeiterinnen der Hochschule werden grundsätzlich als vertrauenswürdig angesehen. Eine 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.

Ungeachtet des oben aufgestellten Vertrauensgrundsatzes ist es erforderlich, die Wirkungsbereiche auf technischer Ebene voneinander abzugrenzen. Damit sollen Fernwirkungen von Fehlfunktionen und Handlungen, die in den Bereich der Sabotage gehören sowie die Folgen eines Einbruchs Unbefugter in IT-Systeme bzw. in das Netz der Hochschule begrenzt werden.

Die IT-Sicherheitsrichtlinien beziehen sich auf alle Aspekte des IT-Einsatzes und legen fest, welche Schutzmaßnahmen zu treffen sind. Nur bei geordnetem Zusammenwirken von technischen, organisatorischen, personellen und baulichen Maßnahmen können drohende Gefahren erfolgreich abgewehrt werden. Welche Schutzmaßnahmen zu treffen sind, ist in der vorliegenden IT-Sicherheitsrichtlinie verbindlich beschrieben.

Für das geordnete Zusammenwirken ist eine Verständigung über die verwendete Terminologie erforderlich. Deshalb werden zunächst (siehe Abschnitt 1.1) die in der IT-Sicherheitsrichtlinie der Hochschule Magdeburg-Stendal enthaltenen zentralen Begriffe erläutert.

Die Beschreibung aller IT-Verfahren (siehe Abschnitt 1.2) ist ein wesentlicher Bestandteil des IT-Sicherheitsprozesses an der Hochschule Magdeburg-Stendal. Den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) folgend, wird unterschieden zwischen Verfahren, deren Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit im Rahmen des Normalmaßes liegen, sowie Verfahren mit höherem Schutzbedarf.

Für die Festlegung des Schutzbedarfs ist eine Schutzbedarfsanalyse (siehe Kapitel 3) durchzuführen. Die zur Erreichung des Grundschutzes erforderlichen Maßnahmen werden unabhängig von den einzelnen Verfahren beschrieben. Der Grundschutz ist unterteilt in einen Bereich für IT-Anwender und für IT-Personal. Als IT-Anwender werden im Folgenden alle Beschäftigten der Hochschule, einschließlich der studentischen Hilfskräfte, verstanden.

Der Begriff IT-Personal bezeichnet alle Beschäftigten der Hochschule Magdeburg-Stendal, deren Tätigkeitsfelder ganz oder überwiegend im Bereich der IT angesiedelt sind (zum Beispiel Administratoren und Applikationsbetreuer).

Die Studierenden der Hochschule Magdeburg-Stendal unterliegen den jeweils geltenden Benutzungsordnungen.

Der für jeden IT-Arbeitsplatz zu erreichende Grundschutz bildet das Fundament der IT-Sicherheit der Hochschule Magdeburg-Stendal. Für IT-Verfahren mit höherem Schutzbedarf müssen über diese Grundschutz-Sicherheitsmaßnahmen hinaus zusätzliche verfahrens- bzw. arbeitsprozessbezogene Maßnahmen erarbeitet werden, die aus entsprechenden Risikoanalysen abgeleitet werden.

Wegen des stetigen Fortschritts auf dem Gebiet der Informationstechnik muss die IT-Sicherheitsrichtlinie regelmäßig überprüft und neuen Anforderungen angepasst werden. Für die Umsetzung der IT-Sicherheitsrichtlinie ist die erfolgreiche Koordination und Überwachung der erforderlichen Aufgaben von entscheidender Bedeutung.

Im Kapitel 1.3 „Verantwortlichkeiten und Organisation der IT-Sicherheit“ wird beschrieben, wie die IT-Sicherheit in den Organisationsstrukturen der Hochschule verankert ist.

2.1. Grundbegriffe der IT-Sicherheitsrichtlinie

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

IT-Arbeitsprozess
Ein IT-Arbeitsprozess ist eine sequenzielle und/oder parallele Abfolge von zusammenhängenden IT-gestützten und/oder IT-unterstützenden Tätigkeiten.

IT-Verfahren
Ein IT-Verfahren ist eine Zusammenfassung von IT-gestützter Arbeitsabläufe. Die zusammengefassten Arbeitsprozesse bilden eine arbeitsorganisatorisch abgeschlossene Einheit und verfolgen ein gemeinsames Ziel. Sie werden beschrieben unter Angabe der technischen und organisatorischen Konzepte und Maßnahmen

Verfügbarkeit
Verfügbarkeit bezieht sich auf Daten und Verfahren und bedeutet, dass Daten und Verfahren bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllen.

Vertraulichkeit
Vertraulichkeit ist eines der vier wichtigsten Sachziele in der Informationssicherheit. Sie wird definiert als „der Schutz vor unbefugter Preisgabe von Informationen.

Integrität
ist ein Schutzziel, das besagt, dass Daten über einen bestimmten Zeitraum vollständig und unverändert sein sollen. Eine Veränderung könnte absichtlich, unabsichtlich oder durch einen technischen Fehler auftreten. *Integrität* umfasst also Datensicherheit (Schutz vor Verlust) und Fälschungssicherheit (Schutz vor vorsätzlicher Veränderung).

Authentizität
Authentizität bedeutet, dass Daten jederzeit und zweifelsfrei ihrem Ursprung zugeordnet werden können.

Revisionsfähigkeit
Revisionsfähigkeit bezieht sich auf die Organisation des Verfahrens. Sie ist gewährleistet, wenn Änderungen an Daten nachvollzogen werden können.

Transparenz
Transparenz ist gewährleistet, wenn das IT-Verfahren für die jeweils Sachkundigen in zumutbarer Zeit mit zumutbarem Aufwand nachvollziehbar ist. In der Regel setzt dies eine aktuelle und angemessene Dokumentation voraus.

Datenschutz
Datenschutz regelt die Verarbeitung personenbezogener Daten, um das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

2.2. IT-Verfahren und Arbeitsprozesse

Ein IT-Verfahren besteht aus einem oder mehreren IT-gestützten Arbeitsprozessen, die eine arbeitsorganisatorisch abgeschlossene Einheit mit einem gemeinsamen Ziel bilden. Die Summe aller IT-Verfahren bildet dann lückenlos den gesamten IT-Einsatz in der Hochschule Magdeburg-Stendal ab.

Mit der Erfassung und Dokumentation aller IT-Verfahren wird der IT-Einsatz in der Hochschule Magdeburg-Stendal vollständig abgebildet.

Einrichtung	**Verfahren**	
Fachbereiche	Foschungsdatenverarbeitung	
	Notenvergabe	
	…	
Dez I	Mittelbewirtschaftung	
	Anlagenbuchhaltung	
	…	
Dez II	Zulassungsverfahren	
	Studierendenorganisation	
	…	
…		
ZKI	Poolbetrieb	
	E-Mail	
	…	

Abbildung 2: Beispiel IT-Verfahren

2.2.1. Erfassung und Dokumentation von IT-Verfahren

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

- Zweck des IT-Verfahrens, Beschreibung der Arbeitsabläufe und Angaben über die gesetzliche Grundlage
- Schutzbedarfsanalyse
- Risikoanalyse in Abhängigkeit vom Ergebnis der Schutzbedarfsanalyse
- Beschreibung der Rollen
- Angaben über die Anzahl und Art von technischen Einrichtungen und Geräten (Mengengerüst)
- Angaben der Schnittstellen zu anderen IT-Verfahren, IT-Systemen und sonstigen Diensten
- Angaben über die vom IT-Verfahren betroffenen Organisationseinheiten
- Aufstellungsort von Anlagen und Geräten, die wesentliche Funktionen innerhalb des Arbeitsprozesses bzw. IT-Verfahrens erfüllen; alle weiteren Anlagen und Geräte müssen lediglich zahlenmäßig erfasst und einer Unterorganisationseinheit zugewiesen werden
- Betriebskonzept mit allen für den Betrieb notwendigen Angaben über die im IT-Verfahren erfassten technischen Systeme
- Soweit personenbezogene Daten der Beschäftigten automatisiert verarbeitet werden: Angaben über den Umgang mit personenbezogenen Daten.

Eine vollständige Auflistung möglicher Inhalte einer IT-Verfahrensbeschreibung befindet sich in der Dienstvereinbarung IT-Sicherheit im § 6 „Dokumentation von IT-Verfahren“.

Abweichend von den vorangegangenen Dokumentationskriterien gilt für den Betrieb von IT-Systemen in Forschungsprojekten und für IT-Systeme mit kurzer Betriebsdauer (weniger als sechs Monate) keine Pflicht zur ausführlichen Verfahrensbeschreibung. Hauptsächlich muss lediglich der Betrieb angezeigt werden. Die in diesem Fall geltenden Regeln sind in der Dienstvereinbarung IT-Sicherheit im § 6 „IT-Systeme in Forschungsprojekten sowie IT-Systeme mit kurzer Lebensdauer“ beschrieben. Auch wenn für IT-Systeme in Forschungsprojekten und für IT-Systeme mit kurzer Betriebsdauer keine Verpflichtung zur Durchführung einer Schutzbedarfsanalyse und ggf. einer Risikoanalyse besteht, muss dennoch die Sicherheit aller betroffenen Systeme sowie der zugrunde liegenden Infrastruktur gewährleistet werden. Beispielsweise können, speziell dafür ausgelegte Netzwerke, die gegenüber anderen Netzwerken abgeschottet sind, bereitgestellt werden. Auch der Einsatz virtueller Serversysteme kann neben anderen Maßnahmen zur Erhöhung der Sicherheit beitragen.

Weitere Merkmale eines IT-Verfahrens sind der längerfristige Charakter der erfassten IT-gestützten Arbeitsabläufe. Ein IT-Verfahren wird üblicherweise über mehrere Jahre hinweg betrieben. Bei der Festlegung von IT-Arbeitsprozessen in IT-Verfahren soll der Grundsatz der Generalisierung bzw. der Zusammenfassung beachtet werden. Der IT-Arbeitsprozess bildet bei der Erfassung des IT-Einsatzes die kleinste Einheit. Als Anhaltspunkt für eine Zusammenfassung oder eine Trennung von Arbeitsabläufen können u. a. folgende Kriterien dienen:

Trennkriterien
- unterschiedlicher Schutzbedarf
- verschiedene Datenkategorien
- verschiedene „Datenbesitzer“

Zusammenfassungskriterien
- Praktikabilität
- Arbeitsersparnis
- Zusammenhängende Aufgaben

Ein oder mehrere Arbeitsprozesse können ein IT-Verfahren bilden, wobei die beteiligten Arbeitsprozesse ein gemeinsames Ziel verfolgen müssen. Die Differenzierung eines IT-Verfahrens in mehrere IT-Arbeitsprozesse ermöglicht, das auch relativ komplexe IT-Verfahren angemessen aus Sicht der IT-Sicherheit, des Datenschutzes und der Mitbestimmung behandelt und analysiert werden können. Außerdem werden damit die zukünftig vom IT-Controlling gestellten Anforderungen an eine strukturierte Darstellung IT-gestützter Geschäftsprozesse erfüllt.

Beispiel IT-Verfahren mit einem Arbeitsprozess: Betrieb eines PC-Pools

Der Betrieb eines PC-Pools beinhaltet typischerweise Tätigkeiten, die alle der Bereitstellung von PCs dienen. Die Aufteilung der Tätigkeiten in verschiedene Arbeitsprozesse ist nicht sinnvoll, da beispielsweise auf die einzelnen Arbeitsprozesse das Rollenmodell nicht mehr sinnvoll angewendet werden kann.

Beispiel IT-Verfahren mit mehreren Arbeitsprozessen: HIS-Module (Hochschulinformationssystem)

Die HIS-Module umfassen eine Vielzahl von zusammenhängenden Prozessen in verschiedenen Organisationseinheiten der Hochschule. Beispielhaft sollen das Rückmelde- und Prüfungsverfahren herangezogen werden.

Rückmeldeverfahren: Zu Beginn eines Semesters müssen sich die Studierenden rückmelden. An diesem Verfahren sind mehrere Dezernate beteiligt, wie Immatrikulationsamt und Mittelbewirtschaftung. In den Dezernaten gibt es mehrere Arbeitsprozesse, die verschiedenen Rollen zuzuordnen sind.

Prüfungsverfahren: In der Regel zum Ende eines Semesters werden die Prüfungsergebnisse erstellt und verwaltet. Auch dieser Prozess ist relativ komplex und beinhaltet eine Reihe von verschiedenen Abläufen in unterschiedlichen Einrichtungen (Prüfungsamt, Fachbereiche) mit verschiedenen Akteuren (Studierende, Mitarbeiter und Mitarbeiterinnen im Prüfungsamt, Dozenten).

In beiden Prozessen werden auch unterschiedliche Daten verarbeitet. Zu einem sind es Stammdaten der Studierenden. Im anderen Fall werden vor allem Prüfungsdaten verarbeitet.

Aus diesen Gründen wäre in diesem Beispiel die Aufteilung in Arbeitsprozesse empfehlenswert. Allgemein gilt, dass es normalerweise nicht sinnvoll ist, einzelne Tätigkeiten, wie z.B. die Erledigung der Korrespondenz, als einen eigenen Arbeitsprozess oder sogar als ein eigenes IT-Verfahren festzulegen. Dadurch würde eine große Zahl von IT-Arbeitsprozessen bzw. -Verfahren entstehen, deren strukturierte Bearbeitung kaum mehr zu leisten ist.

Im jährlichen Turnus, jeweils zum 1. März, sind alle Bereiche, die IT-Verfahren gemeldet haben, zur Aktualisierung der gemeldeten Daten verpflichtet. Dazu muss eine Änderungsmeldung an die durch die Leitung der Hochschule Magdeburg-Stendal beauftragten Stelle, zurzeit das ZKI, erfolgen.

Die Änderungsmeldung muss erfolgen durch die

- Bestätigung des unveränderten Betriebs oder
- Aktualisierung der Verfahrensbeschreibung oder
- Meldung der Einstellung eines IT-Verfahrens.

2.2.2. Rollen

Die Rollenverteilung innerhalb eines IT-Verfahrens orientiert sich an folgendem Rollenmodell.

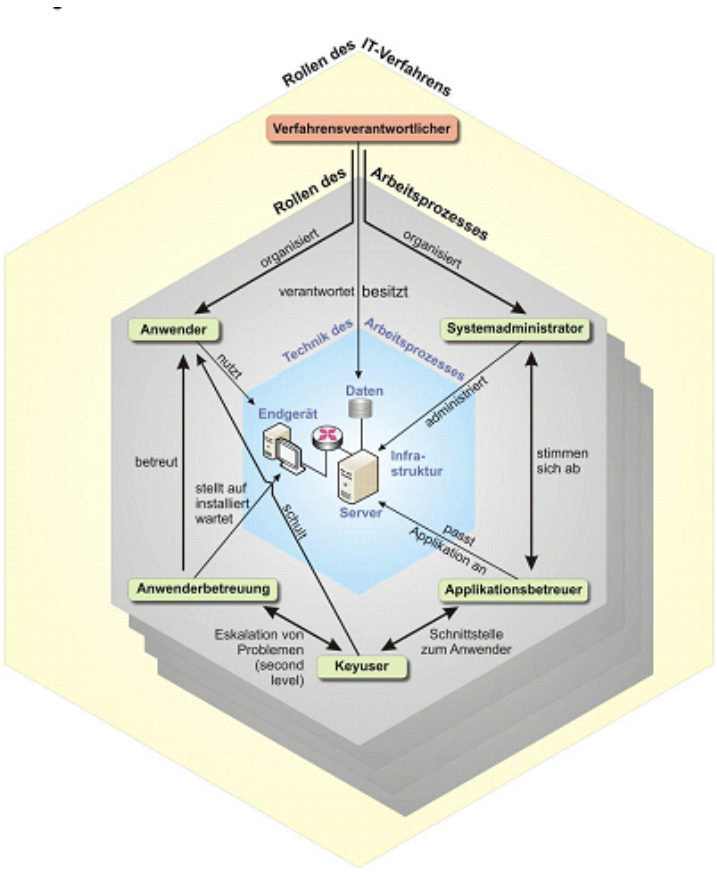

Abbildung 3: Darstellung der wichtigsten Rollen (keine Personen) innerhalb eines IT-Arbeitsprozesses und eines IT-Verfahren. Die dunkelgrau hintereinander geschachtelten Waben sollen andeuten, dass zu einem IT-Verfahren (gelbe Wabe) mehrere IT-Arbeitsprozesse gehören können. Quelle:IT-Sicherheitsrahmenrichtlinie FU Berlin

Eine Rolle kann als Bündelung von Kompetenzen aufgefasst werden, die zur Bearbeitung von Aufgaben innerhalb eines IT-gestützten Prozesses benötigt werden. Eine Rolle beschreibt somit, für welche Aufgaben man mit welchen Rechten auf welche Ressourcen zugreift. Die Rolle der/des Verfahrensverantwortlichen ist für jedes IT-Verfahren zwingend notwendig.

Die konkrete personelle Zuordnung einer Rolle ist abhängig von dem betreffenden IT-Verfahren bzw. IT-Arbeitsprozess. Zum Beispiel kann bei großen und komplexen IT-Arbeitsprozessen die Rolle des/der Applikationsbetreuers/in von mehreren Personen übernommen werden. Anderseits kann bei kleinen IT-Arbeitsprozessen diese Rolle von einer Person übernommen werden, die gleichzeitig auch die Rolle eines/r Anwenderbetreuers/in und/oder Key-Users ausfüllt. Eine Rolle kann also von einer oder mehreren Personen ausgefüllt werden. Andererseits kann aber auch eine Person mehrere Rollen wahrnehmen. Darüber hinaus ist zu beachten, dass nicht alle dargestellten Rollen in einem konkretem IT-Arbeitsprozess zwingend notwendig sind. Beispielsweise ist die Rolle des Key-Users in kleineren IT-Verfahren bzw. IT-Arbeitsprozessen oft nicht vorhanden.

Die an der Hochschule Magdeburg-Stendal verbindliche Beschreibung aller Rollen im IT-Sicherheitsprozess beinhaltet die IT-Sicherheitsordnung der Hochschule Magdeburg-Stendal.

2.3. Verantwortlichkeiten und Organisation der IT-Sicherheit

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

Die für die IT-Sicherheit aus organisatorischer und strategischer Sicht bedeutendsten Rollen sollen an dieser Stelle kurz dargestellt werden:

Hochschulleitung
Die Hauptverantwortung für den IT-Sicherheitsprozess liegt bei der Hochschulleitung. Sie übernimmt grundsätzlich die Rolle des IT-Sicherheitsbeauftragten.

IT-Sicherheitsmanagement-Team (SMT)

Die Hochschulleitung setzt ein IT-Sicherheitsmanagement-Team (SMT) ein. Die Zusammensetzung des SMT sollte – unter Beschränkung der Anzahl der Mitglieder auf das notwendige Maß– sowohl die unterschiedlichen Aufgabenbereiche der Hochschule Magdeburg-Stendal widerspiegeln als auch die unterschiedlichen, für die Hochschule relevanten Aspekte der IT-Sicherheit berücksichtigen. Ständige Mitglieder des SMT sind

i. ein(e) Vertreter(in) der Hochschulleitung,
ii. der/die Datenschutzbeauftragte,
iii. ein(e) Vertreter(in) der dezentralen IT-Sicherheitsbeauftragten (siehe § 3),
iv. Leiter/-in des ZKI,
v. Leiter/-in der Kommission für Kommunikation und Informationsverarbeitung.

Zu den zentralen Aufgaben des SMT gehören:

- IT-Sicherheitsziele und -strategien zu bestimmen sowie die IT-Sicherheitsrichtlinie zu entwickeln,
- den IT-Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
- zu überprüfen, ob die in der IT-Sicherheitsrichtlinie geplanten IT-Sicherheitsmaßnahmen wie beabsichtigt funktionieren also geeignet und wirksam sind,
- bei der Fortschreibung der IT-Sicherheitsrichtlinie mitzuwirken,
- die Schulungs- und Sensibilisierungsprogramme für IT-Sicherheit zu konzipieren sowie
- die Leitungsebene in IT-Sicherheitsfragen zu informieren und zu beraten.

Hierbei werden Datenschutz- und Mitbestimmungsaspekte beachtet.

dezentrale IT-Sicherheitsbeauftragte
Zu den zentralen Aufgaben eines/r IT-Sicherheitsbeauftragten gehören:

- Mitarbeit bei der Erstellung und Umsetzung von bereichsübergreifenden IT-Konzepten,
- Erfassung und Dokumentation des bereichsinternen IT-Einsatzes,
- Koordination von IT-Schulungsmaßnahmen,
- Ansprechpartner für Mitarbeiter/-innen der betreffenden Organisationseinheit in Fragen der IT-Organisation und IT-Sicherheit und
- Ansprechpartner der betreffenden Einrichtung für alle Gremien und andere Organisationseinheiten in Fragen der IT-Organisation und IT-Sicherheit.
- die Realisierung für IT-Sicherheitsmaßnahmen zu initiieren und zu prüfen,
- der Leitungsebene und der AG IT-Sicherheit über den Statuts Quo der IT-Sicherheit zu berichten,
- sicherheitsrelevante Projekte koordinieren,
- Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen.

IT-Personal (IT-Betreuer, Systemadministratoren)
Eine natürliche Person, die administrativen Aufgaben im laufenden IT-Betrieb wahrnimmt. Sie ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems bzw. sie nimmt Benutzeranfragen zu Problemen rund um die IT-Ausstattung entgegen und bearbeitet sie. In der Regel die DV-Organisatoren/-innen der Bereiche.

Rektoratsbeauftragter für IuK
Der/Die Rektoratsbeauftragte für IuK versteht sich als Bindeglied zwischen dem ZKI und der Hochschulleitung bzw. ihren Gremien, der Verwaltung und den Studierenden. Dabei sieht er/sie seine Aufgaben in erster Linie in der Aufrechterhaltung und Vertiefung einer konstruktiven Kommunikation zwischen diesen Bereichen der Hochschule. Dies bezieht sich zum einen auf die Pflege der aktuellen laufenden IuK Architektur sowie auf die Entwicklung einer modernen und zukunftsgerichteten Weiterentwicklung in Abstimmung mit der Hochschulleitung, dem ZKI sowie unter Beobachtung nationaler und internationaler Entwicklungen.

Der/Die IuK Beauftragte übernimmt den Vorsitz einer entsprechenden Kommission des Senates.

IT-Senatskommission
Die vom Senat der Hochschule Magdeburg-Stendal eingesetzte IuK-Kommission berät mit der Leitung des Zentrums für Kommunikation und Informationsverarbeitung(ZKI) den Senat in Fragen von grundsätzlicher Bedeutung, die mit dem Betrieb und den Anschaffungen des Zentrums für Kommunikation und Informationsverarbeitung zusammenhängen.

Zentrale IT-Dienstleister
Zentrale IT-Dienstleister planen, realisieren, betreiben, gestalten und stellen IT-Infrastrukturen und IT-Services für die Einrichtungen der Hochschule bereit. IT-Dienstleister im Sinne dieser Begriffsbestimmung ist das Zentrum für Kommunikation und Informationsverarbeitung (ZKI). Das ZKI ist für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit zentraler Systeme (Systembetreiber lt. §3 Absatz 2.a der „Benutzungsordnung für Informationsverarbeitungssysteme der Fachhochschule Magdeburg“) verantwortlich.

Bereiche der Hochschule
Die Leitung einer Organisationseinheit (Dekan/-in, Dezernent/-in) trägt die Verantwortung für den laufenden IT-Einsatz in ihrem Aufgabenbereich sowie für alle bereichsinternen IT-Planungen. Die Bereichsleitung gibt auf Grund der Ergebnisse der Schutzbedarfs- und ggf. Risikoanalyse den Betrieb des IT-Verfahrens frei. Sie benennt eine/n dezentralen IT-Sicherheitsbeauftragte/n, der/die in ihrem Auftrag den IT-Einsatz koordiniert und plant und darüber hinaus die in der IT-Sicherheitsrichtlinie formulierten Maßnahmen umsetzt.

Verfahrensverantwortlicher
Der/Die IT-Verfahrensverantwortliche trägt die Gesamtverantwortung für ein oder mehrere spezielle IT-Verfahren und ist für den korrekten Ablauf verantwortlich. Er/Sie ist der/die Besitzer/in der im Verfahren verarbeiteten Daten und bestimmt den Schutzbedarf seines/ ihres Verfahrens.

IT-Anwender (Nutzer/in)
Natürliche Person, die/der als Angehörige/r oder Gast der Hochschule Magdeburg-Stendal berechtigt deren IT-Ressourcen verwendet.

3. Definition des Grundschutzes

Sicherheit in der Informationstechnik dient der Sicherstellung von Verfügbarkeit, Integrität und Vertraulichkeit von Daten und IT-Anwendungen. Sie ist nur durch die Bündelung von Maßnahmen aus den Bereichen Organisation, Personal, Infrastruktur, Hard- und Software, Kommunikation und Notfallvorsorge zu erreichen.

Die Schutzwürdigkeit von Daten und Verfahren ist nicht einheitlich. Daher unterscheiden sich auch die jeweils angemessenen Schutzmaßnahmen. Während im medizinischen Bereich bereits ein kurzzeitiger Ausfall der IT Leben in Gefahr bringen kann, bleibt in anderen Bereichen eine längere Ausfallzeit ohne schädliche Auswirkungen. Personaldaten erfordern einen höheren Schutzaufwand als z.B. Raumdaten. Der Schutzbedarf von Ergebnissen wissenschaftlicher Forschung ist in größtem Maße uneinheitlich (siehe Schutzbedarfsanalyse).

Die hier für den Grundschutz zusammengestellten Maßnahmen gewährleisten ausreichende Sicherheit bei normalem Schutzbedarf. Sie bilden die Grundlage für alle IT-Verfahren/ IT-Arbeitsprozesse der Hochschule Magdeburg-Stendal. Ihre Realisierung in den Organisationseinheiten ist notwendige, aber nicht immer hinreichende Voraussetzung für die Teilnahme an übergreifenden IT-Verfahren wie der Nutzung zentraler Dienste, zum Beispiel E-Mail, Internet oder dem Identitätsmanagement der Hochschule Magdeburg-Stendal, um nur einige zu nennen.

Die Einhaltung der Vorgaben ist im Interesse der Aufrechterhaltung eines reibungslosen Rechnerbetriebes von größter Wichtigkeit, denn bereits ein ungeschützter Rechner birgt Gefahren für das gesamte Hochschulnetz. Aus dem Blickwinkel des Nutzers eines einzeln betriebenen Rechners ohne Sicht auf die Folgen für das vernetzte Gesamtsystem mögen die beschriebenen Maßnahmen für die Mitarbeiter und Mitarbeiterinnen möglicherweise unbequem und übertrieben erscheinen. Die Erfahrung zeigt aber, dass die Verbreitung von Schadsoftware über längst bekannte Sicherheitslücken eingesetzter Standardprogramme durch aktuelle Virenscanner und entsprechende Programmaktualisierung verhindert werden kann.

Für IT-Verfahren mit einem **Schutzbedarf „normal“** ist die Umsetzung der Grundschutzmaßnahmen zum Erreichen eines angemessenen Sicherheitsniveaus ausreichend.

Für IT-Verfahren mit **hohem und sehr hohem Schutzbedarf** müssen über diese Grundschutzmaßnahmen hinaus zusätzliche, aus entsprechenden Risikoanalysen abgeleitete und verfahrensbezogene Maßnahmen erarbeitet werden (Zur Erarbeitung von IT-Sicherheitskonzepten für einzelne Verfahren siehe Teil 5 „Umsetzung der IT-Sicherheitsrichtlinie“).

In einigen wenigen Maßnahmen werden über die Erfordernisse des Grundschutzes hinausreichende Handlungsempfehlungen gegeben. Es handelt sich grundsätzlich um Maßnahmen zum Umgang mit besonders schützenswerten Daten.

Die Maßnahmen des Grundschutzes werden gesondert für IT-Anwender/-innen und für IT-Personal dargestellt. Der Maßnahmekatalog ist allen Anwendern/-innen der Hochschule Magdeburg – Stendal in geeigneter Weise bekannt zu geben.

Die Maßnahmen des Grundschutzes für IT-Personal wenden sich unter anderem an IT-Betreuer/innen und Systemadministratoren/innen, die darin Vorgaben für ihre Arbeit finden. Als Basis für die hier dargestellten IT-Grundschutzmaßnahmen dienen die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die dort beschriebenen Maß-

nahmen wurden den Besonderheiten der Hochschule Magdeburg-Stendal angepasst. Bei Fragen zu einzelnen Maßnahmen werden die detaillierten Ausführungen in den IT-Grundschutzkatalogen bzw. die Erläuterungen in der Broschüre „Informationen zum IT-Grundschutz“ empfohlen. Insbesondere beinhalten die BSI-Grundschutzkataloge detaillierte Ausführungen zur Konfiguration von unterschiedlichen Servertypen. Daher wurde auf die detaillierte Behandlung der verschiedenen Servertypen verzichtet.

Zum Zweck der Zuordnung von Verantwortlichkeiten sind zu jeder Regel und zu jeder Maßnahme die Verantwortlichen für die Initiierung und die Verantwortlichen für die Umsetzung benannt. Bei der Initiierung muss unterschieden werden zwischen dem/der bereichsweise zuständigen IT-Sicherheitsbeauftragten und dem/der Verfahrensverantwortlichen. „Verantwortlich für die Initiierung“ bezeichnet die Personen (Rolleninhaber), die die Implementierung einer Maßnahme veranlassen sollen. „Verantwortlich für die Umsetzung“ bezeichnet die Personen (Rolleninhaber), die die Realisierung der Maßnahme in der täglichen Praxis durchführen sollen.

Auf die Behandlung einiger Sicherheitsmaßnahmen zu speziellen Themen wird bewusst verzichtet. Maßnahmen, die sich mit der Absicherung von Rechenzentren beschäftigen werden nicht aufgeführt, weil es an der Hochschule Magdeburg-Stendal nur eine derartige Einrichtung gibt und dementsprechend nur wenige Mitarbeiter und Mitarbeiterinnen von dieser Thematik betroffen sind.

Aus dem gleichen Grund wird auch nicht näher auf Aspekte der Netzinfrastruktur eingegangen. Die Pflege und Wartung aller bereichsübergreifenden Netze ist in dem ZKI bei der dort zuständigen Arbeitsgruppe konzentriert, so dass auch hier wieder nur wenige Mitarbeiter und Mitarbeiterinnen betroffen sind.

Die besondere Problematik in Zusammenhang mit der Einrichtung und Nutzung häuslicher IT-Arbeitsplätze wird zurzeit an der Hochschule Magdeburg-Stendal diskutiert. Unter welchen Bedingungen und in welchem Umfang häusliche IT-Arbeitsplätze genutzt werden dürfen, ist noch nicht abschließend geklärt. Ohne Kenntnis der Rahmenbedingungen ist es deshalb nicht sinnvoll, Maßnahmen zur Sicherheit zu formulieren.

3.1. Maßnahmen des IT-Grundschutzes für IT-Anwender

3.1.1. Allgemeine Maßnahmen IT-Anwender

- **Anwenderqualifizierung (M1.1)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte (bereichsspezifisch), Verfahrensverantwortliche (verfahrensspezifisch)
  Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragte (bereichsspezifisch), Verfahrensverantwortliche (verfahrensspezifisch)

  Die Mitarbeiter und Mitarbeiterinnen sind aufgabenspezifisch zu schulen und dürfen erst dann in IT-Verfahren arbeiten. Dabei sind sie insbesondere auch mit den für sie geltenden Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes vertraut zu machen.

- **Meldung von Sicherheitsproblemen (M1.2)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragte
  Verfahrensverantwortliche

  Auftretende Sicherheitsprobleme aller Art (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u.ä.) sind dem zuständigen IT-Personal mitzuteilen.

3.1.2. Sicherung der Infrastruktur

- **Räumlicher Zugangsschutz (M1.3)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Der unbefugte Zugang zu Geräten und die Benutzung der Informationstechnik muss verhindert werden. Bei Abwesenheit sind Büroräume mit Informationstechnologie verschlossen zu halten. Bei der Anordnung und baulichen Einrichtung der Geräte ist darauf zu achten, dass schützenswerte Daten nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

- **Brandschutz (M1.4)**
  Verantwortlich für Initiierung: Brandschutzbeauftragte, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: Brandschutzbeauftragte, Dezernat IV

  Alle Maßnahmen und Einrichtungen, die dem vorbeugenden Brandschutz dienen, sind einzuhalten bzw. zu nutzen. Lüftungsöffnungen an den Geräten dürfen nicht verstellt oder verdeckt werden. In allen Räumen, in denen Server und Netzwerkkomponenten untergebracht sind, sind alle Tätigkeiten zu unterlassen, die zu einer Rauchentwicklung führen.

- **Sicherung mobiler Computer (M1.5)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, IT-Verantwortliche
  Verantwortlich für Umsetzung: IT-Anwender/-innen

  Bei der Speicherung von schutzbedürftigen Daten auf tragbaren IT-Systemen (Laptops. PDAs, Smartphones etc.) und auf mobilen Datenträgern (z. B. Disketten, CDs, DVDs oder USB-Sticks), die auf Grund ihrer Bauart leicht gestohlen werden können, sind besondere Schutzmaßnahmen (Verschlüsselung) zu treffen, um ein unberechtigtes Auslesen dieser Daten zu verhindern.

  Bei kurzen Arbeitsunterbrechungen muss unbedingt ein Zugriffsschutz - wie im Abschnitt Abmelden und ausschalten (M 1.9) beschrieben - aktiviert werden.

  Um einen tragbares IT-System vor Diebstahl zu schützen, sollten die Zeiten, in denen das Gerät unbeaufsichtigt bleibt, minimiert werden. Geräte die über einen gewissen Zeitraum unbeaufsichtigt sind, sind mit geeigneten Mitteln anzuschließen (z.Bsp. Kensigton-Schloß).

3.1.3. Hard- und Software

- **Kontrollierter Softwareeinsatz (M1.6)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, IT-Verantwortliche
  Verantwortlich für Umsetzung: IT-Anwender/-innen

  Auf Rechnersystemen der Hochschule Magdeburg-Stendal darf nur Software aus vertrauenswürdigen Quellen bezogen, installiert und genutzt werden. die von der jeweils zuständigen Stelle dafür freigegeben wurde (Admins/ IT-Verantwortliche der Bereiche, ZKI). Das eigenmächtige Einspielen oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn eine Genehmigung der zuständigen Stelle vorliegt oder ein Bereich eine pauschale Freigabe für Teilbereiche festgelegt hat. In diesem Fall gelten alle Regelungen für IT-Personal (2.2) entsprechend.

- **Einsatz von privater Hard- und Software (M1.7)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, IT-Verantwortliche
  Verantwortlich für Umsetzung: IT-Anwender/-innen

  Der Einsatz von privater Hard- und Software im Bereich Forschung und Lehre richtet sich im Allgemeinen nach den fachbereichsinternen Regelungen. Bei Fehlen entsprechender Regelungen ist nur hochschuleigene Hard- und Software einzusetzen werden. In speziell gekennzeichneten Bereichen, wie z.B. im Bereich des Wireless LAN der Hochschule, ist der Einsatz von privater Hard- und Software erlaubt.

  In besonders geschützten Bereichen und im Umgang mit Verwaltungsdaten, wie z. Bsp. alle personenbezogenen Daten der Beschäftigten und Studierenden und Daten der Hochschulverwaltung, ist die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der Hochschule Magdeburg-Stendal und deren Netzen grundsätzlich nicht gestattet. Ausnahmen regelt das SMT.

- **Schutz vor Schadprogrammen (M1.8)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, IT-Verantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Auf allen Arbeitsplatz-PCs ist ein aktuelles Malware-Schutzprogramm einzurichten, das automatisch alle eingehenden und zu öffnenden Dateien überprüft. Damit soll bereits das Eindringen von schädlichen Programmen (Viren, Würmer, Dialer, Spyware,….) erkannt und verhindert werden. Wenn aus technischen Gründen die Installation von Schutzprogrammen nicht möglich ist (zum Beispiel bei Prozessrechnern mit Netzanschluss), müssen alternative Schutzmaßnahmen, beispielsweise die Abschottung von Netzsegmenten, ergriffen werden.

  Beim Verdacht auf Infektion mit Malware ist in jedem Falle das zuständige IT-Personal zu informieren. Neben der Meldung durch Schutzprogramme können unerklärliches Systemverhalten, ungewöhnlich hoher Ressourcenverbrauch oder unerwartete Netz-zugriffe Anzeichen für einen Malwarebefall sein.

  Informationen zum Malwareschutz finden sich unter
  http://www.zki.hs-magdeburg.de/dienste/sicherheit/viren .

3.1.4. Zugriffsschutz

- **Abmelden und ausschalten (M1.9)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Bei längerer Abwesenheit muss sich der/die Benutzer/in aus den laufenden Anwendungen und dem Betriebssystem abmelden. Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen, die nur durch eine erfolgreiche Benutzerauthentifizierung, also z. Bsp. eine Passwortabfrage, deaktiviert werden kann. Zusätzlich ist sollte die Bildschirmsperre nach einem vorgegebenen Inaktivitäts-Zeitraum von 10 Minuten automatisch gestartet werden.

  Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen.

- **Personenbezogene Kennungen (M1.10)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Alle IT-Systeme sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine persönliche Anmeldung mit Benutzerkennung und Passwort oder einem anderen Authentifizierungsverfahren erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen erfolgt in der Regel personenbezogen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem/Der Benutzer/in ist untersagt, Kennungen und Passwörter weiterzugeben.

- **Gebrauch von Passwörtern (M1.11)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Der/Die Benutzer/in hat sein/ihr Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden. Sofern die technischen Gegebenheiten dies zulassen, sind Passwörter nach den folgenden Regeln zu gestalten:
  - Das Passwort muss mindestens 8 Stellen lang sein.
  - Das Passwort muss mindestens einen Buchstaben und mindestens eine Ziffer oder ein Sonderzeichen enthalten.
  - Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln und sollte eine Mindestgültigkeitsdauer von einem Tag haben.
  - Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.

  Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt. Erhält ein/e Benutzer/in beim Anmelden mit seinem/ihrem Passwort keinen Zugriff auf das System, besteht die Gefahr, dass sein/ihr Passwort durch Ausprobieren ermittelt wurde, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem/der zuständigen Vorgesetzten und dem IT-Personal zu melden. (Siehe M1.2). Bei Vergessen des Passwortes bzw. nach mehrfacher fehlerhafter Passworteingabe hat der/die Benutzer/in die für diesen Fall vorgesehene Verfahrensweise zu befolgen. Die Zahl der erlaubten Fehlversuche wird von der zuständigen Stelle festgelegt. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird. In vielen Systemen muss das Zurücksetzen des Passworts durch den/die Administrator/in veranlasst werden. Andere Systeme sehen für diesen Fall vor, dass der/die Benutzer/in sich selbst wieder registriert.

- **Zugriffsrechte (M1.12)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Verantwortliche

  Der/Die Benutzer/in darf nur mit den Zugriffsrechten ausgestattet werden, die unmittelbar für die Erledigung seiner/ihrer Aufgaben vorgesehen sind. Im Bereich der Hochschulverwaltung erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer/innen auf schriftlichen Antrag. In allen anderen Organisationseinheiten sind die dort geltenden Regelungen zu beachten.

- **Netzzugänge (M1.13)**
  Verantwortlich für Initiierung: IT-Sicherheitsmanagement- SMT
  Verantwortlich für Umsetzung: IT-Verantwortliche, IT-Sicherheitsbeauftragte

  Der Anschluss von Systemen an das Datennetz der Hochschule Magdeburg-Stendal hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (WLAN-Access-Points, Modems, Bridge's, o. ä.) ist grundsätzlich verboten. Ausnahmen regelt das SMT.

3.1.5. Kommunikationssicherheit

- **Sichere Netzwerknutzung (M1.14)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Der Einsatz von verschlüsselten Kommunikationsdiensten ist, nach Möglichkeit, den unverschlüsselten Diensten vorzuziehen. Schutzbedürftige Daten sind immer verschlüsselt zu übertragen.

3.1.6. Datensicherung

- **Datensicherung (M1.15)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Regelmäßig durchgeführte Datensicherungen sollen vor Datenverlust schützen. Grundsätzlich sind Daten auf zentralen Servern zu speichern. Ist die Sicherung auf zentralen Servern noch nicht möglich, ist der/die Benutzer/in für die Sicherung seiner/ihrer Daten selbst verantwortlich.

  Informationen zum Backup-Service des ZKI finden sich unter
  http://www.zki.hs-magdeburg.de/dienste/tsm .

3.1.7. Umgang mit Datenträgern

- **Sichere Aufbewahrung (M1.16)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Mobile Datenträger mit schützenswerten Daten sind so aufzubewahren, dass zum einen ein unbefugter Zugriff durch die Verwendung geeigneter, verschlossener Behältnisse, Schränke, Räume verhindert wird und zum anderen die Lagerungsbedingungen gemäß den Herstellerangaben eingehalten werden. Insbesondere ist darauf zu achten, dass ein hinreichender Schutz gegen Magnetfelder und Staub, sowie eine klimagerechte Lagerung gewährleistet ist.

- **Datenträgerkennzeichnung (M1.17)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Alle mobilen Datenträger, auf denen schützenswerte Daten dauerhaft gespeichert werden, sind soweit möglich eindeutig zu kennzeichnen. Aus der Beschriftung soll die Verwendung (Verfahren, Dateien, Inhalt), Datum der ersten Ingebrauchnahme sowie das Datum des letztmaligen Beschreibens hervorgehen. Bei besonders schützenswerten Daten ist die Beschriftung so zu wählen, dass ein Rückschluss auf den Inhalt für Unbefugte nicht möglich ist.

- **Gesicherter Transport (M1.18)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Die Übermittlung von Datenträgern mit schützenswerten Daten hat persönlich, per Kurier, per Wertbrief oder mit vergleichbaren Transportdiensten zu erfolgen. Während des Transports müssen sich die Datenträger in einem verschlossenen Behältnis befinden, dessen unbefugte Öffnung festgestellt werden kann. Die Weitergabe dieser Datenträger erfolgt nur gegen Quittung.

- **Physisches Löschen von Datenträgern (M1.19)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Geeignete Werkzeuge und Anleitungen werden vom ZKI bereitgestellt. Ggf. ist auch hier die mechanische Zerstörung anzuwenden.

  Eine Fremdentsorgung ist möglich. Hier ist eine sorgfältige Auswahl des Auftragnehmers notwendig (datenschutzrechtliche Aspekte).

3.1.8. Schützenswerte Daten

- **Schützenswerte Daten auf dem Arbeitsplatz-PC (M1.20)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Das Speichern schützenswerter Daten auf der Festplatte des Arbeitsplatz-PCs oder anderer lokaler Speicher- oder Übertragungsmedien und deren Übertragung ist nur verschlüsselt zulässig. Die Zugriffsrechte der verschlüsselten Dateien sind so zu setzen, dass Unbefugte keinen Zugriff erlangen können.

3.2.Maßnahmen des IT-Grundschutzes für IT-Personal

Die im Folgenden beschriebenen Maßnahmen richten sich an alle Mitarbeiter und Mitarbeiterinnen der Hochschule Magdeburg-Stendal, die verantwortlich Aufgaben im IT-Betrieb wahrnehmen oder Verantwortung im organisatorischen Bereich tragen. Insbesondere sind dies DV-Verantwortliche, Verfahrensverantwortliche, System- und Netzadministratoren, Applikationsbetreuer, Benutzerservice, Programmentwickler u.a. Die im vorangegangenen Abschnitt dargestellten Maßnahmen für die IT-Anwender werden hier vorausgesetzt. Im Interesse einer möglichst übersichtlichen Darstellung werden einige Maßnahmen wiederholt, wobei sie gelegentlich weiter ausgeführt oder erweitert werden. Bei spezifischen Aufgabenstellungen, insbesondere im Umfeld von System- und Netzadministration, kann eine Abweichung in einzelnen Punkten der zuvor behandelten Maßnahmen notwendig sein. In jedem Fall ist aber der zugrunde liegende Sicherheitsgedanke nicht außer Kraft zu setzen, sondern der gegebenen Situation anzupassen.

3.2.1. Allgemeine Maßnahmen IT-Personal

- **Grundsätze für den IT-Einsatz (M2.1)**
  Verantwortlich für Initiierung: Hochschulleitung
  Verantwortlich für Umsetzung: Bereichsleitung, IT-Sicherheitsmanagement- SMT

  Beschaffung, Entwicklung und Einsatz von IT-Anwendungen und -Systemen erfolgt nach Maßgabe der für die Hochschule geltenden Regelungen. Zusätzlich sind Regelungen des Bundes und des Landes Sachsen-Anhalt zu beachten, die eine ordnungsgemäße IT-Organisation, Verfahrensplanung und -realisierung beschreiben, soweit diese für die Hochschule Magdeburg–Stendal verbindlich sind.

  IT-Sicherheitsaspekte sind bereits zu Beginn eines Projektes (z.B. bei Anschaffung neuer Software oder bei Planung von Geschäftsprozessen) zu berücksichtigen.

- **Gesamtverantwortung (M2.2)**
  Verantwortlich für Initiierung: Hochschulleitung, SMT
  Verantwortlich für Umsetzung: Bereichsleitung

  Die Verantwortung für die Umsetzung und Einhaltung der für den IT-Einsatz geltenden Regelungen tragen die einzelnen Bereichsleitungen (Dekanate, Leitungen) in den Fachbereichen, Zentralen Einrichtungen und der Hochschulverwaltung entsprechend den Regelungen des Hochschulgesetzes des Landes Sachsen-Anhalt.

3.2.2. Organisation von IT-Sicherheit

- **Beschreibung von IT-Verfahren (M2.3)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: Verfahrensverantwortliche

  Der gesamte IT-Einsatz ist in IT-Verfahren zu gruppieren. Jedes Verfahren ist zu beschreiben. Anforderungen an die Beschreibung sind in der Dienstvereinbarung IT-Sicherheit festgelegt. Im Abschnitt 1.2 dieser Richtlinie wurden die wichtigsten Aspekte einer Verfahrensdokumentation zusammengefasst.

- **Rollentrennung (M2.4)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Für jedes IT-Verfahren bzw. jeden IT-Arbeitsprozess sind die Verantwortlichkeiten für alle Bereiche eindeutig festzulegen. Normalerweise ist eine Rollentrennung von Verfahrensentwicklung/-pflege und Systemadministration sinnvoll. Jedem Mitarbeiter und jeder Mitarbeiterin müssen die ihm/ihr übertragenen Verantwortlichkeiten und die ihn/sie betreffenden Regelungen bekannt sein. Abgrenzungen und Schnittflächen der verschiedenen Anwenderrollen müssen klar definiert sein.

- **Benennung eines IT-Sicherheitsbeauftragten (M2.5)**
  Verantwortlich für Initiierung: Hochschulleitung, SMT
  Verantwortlich für Umsetzung: Bereichsleitung

  Den dezentralen IT-Sicherheitsbeauftragten der Organisationseinheiten kommt im Rahmen der IT-Sicherheitsrichtlinie der Hochschule eine zentrale Bedeutung zu, denn sie haben in ihrem Zuständigkeitsbereich die für den IT-Einsatz gebotenen technischen und organisatorischen Maßnahmen zur IT-Sicherheit zu initiieren und zu koordinieren. Sie führen die notwendigen Aufzeichnungen für die Organisationseinheit ihrer Zuständigkeit. Bei Fragen des IT-Einsatzes sind sie sowohl Ansprechpartner für die Mitarbeiter und Mitarbeiterinnen ihrer Organisationseinheit als auch für Dritte (außerhalb ihrer Organisationseinheit)

- **Dokumentation der IT-Verfahren bezüglich der IT-Sicherheit (M2.6)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte,Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal

  IT-Verfahren sind bezüglich Sicherheit mindestens zu folgenden Punkte zu dokumentieren:
  - Zweck des IT-Verfahrens, Zielsetzung, Begründung und Beschreibung der Arbeitsabläufe
  - Schutzbedarfsanalyse mit einer Bewertung auf Grundlage der in dieser Richtlinie dargestellten Bewertungstabelle
  - Ggf. Risikoanalyse in Abhängigkeit vom Ergebnis der Schutzbedarfsanalyse
  - Beschreibung der Rollen; ggf. in Form eines Berechtigungskonzepts
  - Vertretungsregelungen, insbesondere im Administrationsbereich
  - Zugriffsrechte
  - Organisation, Verantwortlichkeit und Durchführung der Datensicherung
  - Notfallregelungen
  - Ggf. Wartungsvereinbarungen
  - Ggf. Verfahrensbeschreibungen nach Datenschutzrecht

  Darüber hinaus sind die Regelungen der bestehenden Dienstvereinbarung IT-Sicherheit zur Dokumentation von IT-Verfahren zu beachten. Nur dokumentierte Verfahren dürfen betrieben werden. Der/Die dezentrale IT-Sicherheitsbeauftragte ist verantwortlich für die aktuelle Dokumentation der Verfahren seiner Organisationseinheit. Verfahrensverantwortliche, Systemadministratoren/-innen und Applikationsbetreuer/-innen sind dabei durch die IT-Sicherheitsordnung zur Mitarbeit verpflichtet.

- **Dokumentation von Ereignissen und Fehlern (M2.7)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Ereignisse, die Indiz für ein Sicherheitsproblem sein können, sind dem Betreiber des betroffenen Systems zu melden. Sie können außerdem für die Fortschreibung der IT-Sicherheitsrichtlinie wertvolle Hinweise liefern und sind daher zu dokumentieren. Zu erfassen sind z.B. Systemabstürze, Hardwareausfälle sowie das Eindringen Unbefugter. Zuständig für die Dokumentation ist der/die Rollenträger/in, in dessen/deren Aufgabengebiet das Ereignis eingetreten ist. Der IT-Sicherheitsbeauftragte organisiert die Vollständigkeit der Meldungen zu sicherheitsrelevanten Ereignissen in seiner Dokumentation und reicht die Meldungen an das SMT weiter, die für die Fortschreibung der IT-Sicherheitsrichtlinie relevant sein könnten.

- **Regelungen der Auftragsdatenverarbeitung (M2.8)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: Verfahrensverantwortliche

  Für alle im Auftrag der Hochschule Magdeburg-Stendal betriebenen IT-Verfahren ist eine schriftliche Vereinbarung Voraussetzung. Die Verantwortung für die IT-Sicherheit ist eindeutig zuzuweisen und entsprechende Kontrollmöglichkeiten vorzusehen. Sofern im Rahmen der Auftragsdatenverarbeitung personenbezogene Daten verarbeitet werden, sind die entsprechenden Regelungen des Datenschutzgesetzes des Landes Sachsen-Anhalt zu beachten (gilt auch für Wartungsarbeiten).

- **Standards für technische Ausstattung (M2.9)**
  Verantwortlich für Initiierung: Hochschulleitung, SMT
  Verantwortlich für Umsetzung: ZKI

  Zur Erreichung eines ausreichenden Sicherheitsniveaus für IT-Systeme sind Qualitätsstandards im Sinne dieser Richtlinie vom ZKI unter Maßgabe der vom IT-Sicherheitsmanagement-Team (SMT) definierten Strategien zu formulieren und regelmäßig neuen Anforderungen anzupassen. Bei der Entwicklung der Standards sind die spezifischen Bedürfnisse der Fachbereiche zu berücksichtigen.

- **Revision der Sicherheit (M2.10)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Verantwortliche, IT-Personal

  Alle eingesetzten IT-Sicherheitsmaßnahmen müssen auf ihre Tauglichkeit, Wirksamkeit und Einhaltung überprüft werden. Diese Überprüfung muss regelmäßig und nach jeder Änderung der Sicherheitsstandards erfolgen. Dies kann mit Hilfe entsprechender Tools im ZKI selbst oder durch externe Dienstleister durchgeführt werden (Anbieter möglichst mit Zertifikaten des BSI)

- **Allgemeine Notfallvorsorge (M2.11)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragter
  Verantwortlich für Umsetzung: IT-Verantwortliche, IT-Personal

  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 sollte ein Notfallplan erstellt werden, in dem festgelegt wird, wie auf Notfallsituationen adäquat reagiert wird. „Notfall“ bezeichnet eine Situation, in der durch eine Betriebsstörung die Verfügbarkeit, Integrität oder Vertraulichkeit der Daten nicht mehr gegeben ist und ein verhältnismäßig hoher Schaden entsteht. In einem Notfallplan sollten zum Beispiel Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten und zum Einsatz von Ausweichmöglichkeiten enthalten sein. Darüber hinaus ist es häufig sinnvoll einen Alarmierungsplan zu erstellen, in dem die Meldewege im Notfall beschrieben sind.

- **Zentralisierung wichtiger Serviceleistungen (M2.12)**
  Verantwortlich für Initiierung: Hochschulleitung/Rektoratsbeauftragte/r für IT
  Verantwortlich für Umsetzung: ZKI

  Ein leistungsfähiger Nutzerservice, zentral gesteuerte Datensicherungsmaßnahmen, die Möglichkeit der Ablage von Daten auf zentrale File-Server sowie die Möglichkeit der Ausführung von Programmen auf Applikationsservern sind wesentliche Voraussetzungen für einen sicheren und reibungslosen IT-Einsatz zur Unterstützung der täglichen Arbeitsprozesse. Die Softwareverteilung inkl. -installation und –inventarisierung sollte mit Unterstützung entsprechender Werkzeuge erfolgen. Malwareschutz und Firewall-Einsatz sind ebenfalls zu zentralisieren. Beim Einsatz netzwerkweit operierender Installations- und Inventarisierungswerkzeuge sind besondere Maßnahmen zum Schutz vor Missbrauch zu ergreifen. Insbesondere müssen verbindliche Regelungen getroffen werden, die sicherstellen, dass die Werkzeuge ausschließlich für diesen Zweck eingesetzt werden. Dazu muss u. a. festgelegt sein, dass die Werkzeuge nur auf dafür bestimmten, besonders abgesicherten Arbeitsplätzen eingesetzt werden. Der Personenkreis, der berechtigt ist, diese Werkzeuge zu nutzen, ist auf das notwendige Maß zu beschränken. Die Anwender/innen sind vor dem Einsatz solcher Werkzeuge zu informieren. Ihr Einsatz muss protokolliert und dokumentiert werden.

3.2.3. Personelle Maßnahmen

Zahlreiche Untersuchungen und Statistiken über Fehlfunktionen im IT-Bereich zeigen, dass die größten Risiken durch Irrtum, menschliches Versagen und Überforderung der Mitarbeiter und Mitarbeiterinnen entstehen. Daher sind die in diesem Abschnitt aufgeführten Maßnahmen vorrangig zu beachten.

- **Sorgfältige Personalauswahl (M2.13)**
  Verantwortlich für Initiierung: Bereichsleitung
  Verantwortlich für Umsetzung: Bereichsleitung

  Mit Administrationsaufgaben auf Netzwerk- und Systemebene dürfen nur ausgewählte, ausreichend qualifizierte, vertrauenswürdige und motivierte Mitarbeiter und Mitarbeiterinnen betraut werden.

- **Angemessene Personalausstattung (M2.14)**
  Verantwortlich für Initiierung: Bereichsleitung, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: Bereichsleitung

  Eine zuverlässige und sichere Erfüllung der IT-Aufgaben erfordert eine angemessene Personalausstattung, insbesondere in Hinblick auf die Sicherstellung eines kontinuierlichen Betriebs und der entsprechenden Vertretungsregelungen. Dabei spielen System- und Netzwerkadministratoren/innen eine besondere Rolle.

- **Vertretung (M2.15)**
  Verantwortlich für Initiierung: Bereichsleitung, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: Bereichsleitung

  Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personalausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen.

  Da dem/der Administrator/-in hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle zukommt, muss auch bei seinem/ihrem Ausfall die Weiterführung seiner/ihrer Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter/-innen über die erforderlichen Kenntnisse und Befähigungen verfügen, den aktuellen Stand der Systemkonfiguration kennen, sowie im Bedarfsfall sofort (aber auch erst dann) Zugriff auf die für die Administration benötigten Zutritts-, Zugangs- und Zugriffsberechtigungen haben.

  Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist. Die durch die Vertretung zu erledigenden Aufgaben und die ihr eingeräumten Kompetenzen müssen klar festgelegt sein.

- **Qualifizierung (M2.16)**
  Verantwortlich für Initiierung: Bereichsleitung, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: Bereichsleitung

  IT-Personal darf erst nach ausreichender Schulung mit IT-Verfahren/IT-Arbeitsprozessen arbeiten. Es muss sichergestellt sein, dass die ständige Fortbildung des IT-Personals in allen ihr Aufgabengebiet betreffenden Belangen erfolgt.

3.2.4. Sicherung der Infrastruktur

- **Sicherung von Serverräumen (M2.17)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Verantwortliche, Dezernat IV

  Alle Rechnersysteme mit typischer Serverfunktion, einschließlich der Peripheriegeräte (Konsolen, externe Platten, Laufwerke u. ä.), sind in separaten, besonders gesicherten Räumen aufzustellen. Der Zugang Unbefugter zu diesen Räumen muss zuverlässig verhindert werden.

  Serverräume, in denen besonders schützenswerte Daten gespeichert bzw. verarbeitet werden und die nicht über entsprechende bauliche Sicherungsvorkehrungen verfügen, sollen möglichst unauffällig sein, d. h. Hinweisschilder u. ä. sollten nicht angebracht werden, damit die Funktion der Räume nicht sofort erkennbar wird. Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; verwendete Schlüssel müssen kopiergeschützt sein. Für die Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen. 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. Reinigungspersonal soll die Serverräume nach Möglichkeit nur unter Aufsicht betreten.

- **Geschützte Aufstellung von IT-Endgeräten (M2.18)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragte

  Der unbefugte Zugang zu Geräten und die unbefugte Benutzung von IT-Systemen muss verhindert werden. Bei Abwesenheit des IT-Personals sind Räume mit IT verschlossen zu halten. Es muss gewährleistet sein, dass Schlüssel nur an die jeweils berechtigten Personen ausgegeben werden.

- **Sicherung der Netzknoten (M2.19)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: ZKI

  Netzinfrastruktur (Switches, Router) 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 M2.18.

- **Verkabelung und Funknetze (M2.20)**
  Verantwortlich für Initiierung: SMT, ZKI
  Verantwortlich für Umsetzung: ZKI

  Die Verkabelung des LAN ist klar zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Netzwerkadministratoren müssen einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung zentraler Komponenten haben. Nicht benutzte Anschlüsse sollten abgeklemmt oder deaktiviert werden.

  Erweiterungen und Veränderungen an der Gebäudeverkabelung, auch die Inbetriebnahme von Funknetzen (WLAN), sind Hoheitsaufgaben des ZKI.

- **Einweisung und Beaufsichtigung von Fremdpersonal (M2.21)**
  Verantwortlich für Initiierung: HS-Leitung, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: Bereichsleitung, IT-Sicherheitsbeauftragte

  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 den Umgang mit IT belehrt werden. Wenn bei Arbeiten durch externe Firmen, zum Beispiel im Rahmen der Fernwartung, die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, müssen diese Personen gemäß Datenschutzgesetz auf das Datengeheimnis verpflichtet sein.

- **Stromversorgung und Überspannungsschutz (M2.22)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte,
  Verfahrensverantwortliche
  Verantwortlich für Umsetzung: ZKI, IT-Personal, Dezernat IV

  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 Dezernat IV – Technik, Bau und Liegenschaften herzustellen. Bei Einsatz von Geräten mit redundant ausgelegter Stromversorgung ist darauf zu achten, dass die einzelnen Netzteile nach Möglichkeit über getrennt abgesicherte Stromkreise versorgt werden.

- **USV (M2.23)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verfahrensverantwortliche
  Verantwortlich für Umsetzung: ZKI, IT-Personal

  Alle IT-Systeme, die wichtige oder unverzichtbare Beiträge zur Aufrechterhaltung eines geordneten Betriebes leisten, wie zum Beispiel Server und aktive, zentrale Netzwerkkomponenten, 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.

- **Brandschutz (M2.24)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: Dezernat IV, ZKI, IT-Personal

  Insbesondere in Räumen mit wichtiger Informationstechnik, wie beispielsweise Serverräumen, sind die Brandlasten zu minimieren. Verbrauchsmaterial, leere Verpackungen und andere leicht entflammbare Materialen dürfen in diesen Räumen nicht gelagert werden. Die Türen zu diesen Räumen sollen brandhemmend ausgelegt sein.

  Außerdem sind Brandmelder und Handfeuerlöscher (Brandklasse B mit Löschgas) vorzusehen. Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind.

  Es sollte regelmäßig eine Brandschutzbegehung stattfinden.

- **Schutz vor Wasserschäden (M2.25)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: Dezernat IV, ZKI, IT-Personal

  IT-Systeme, die wichtige oder unverzichtbare Komponenten zur Aufrechterhaltung eines geordneten Betriebes darstellen, sind nicht in direkter Nähe zu oder unter wasserführenden Leitungen aufzustellen. Auch bei Hochwassersituationen muss der weitere Betrieb der IT-Systeme gewährleistet sein. Aus diesem Grund dürfen in hochwassergefährdeten Bereichen IT-Systeme keinesfalls in Kellerräumen aufgestellt werden.

- **Klimatisierung (M2.26)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Bereichsleitung
  Verantwortlich für Umsetzung: Dezernat IV, ZKI, IT-Personal

  Um den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes manchmal nicht aus, so dass der Einbau einer Klimatisierung erforderlich ist. Um die Schutzwirkung aufrecht zu erhalten, ist eine regelmäßige Wartung der Klimatisierungseinrichtung vorzusehen. Eine zusätzliche Überwachungseinrichtung für die Klimatisierung ist vorzusehen. Da bei einem Ausfall der Klimatisierung unter Umständen viele (insbesondere wichtige) IT-Systeme abgeschaltet werden müssen, sollte diese auf eine hohe Verfügbarkeit ausgelegt sein.

3.2.5. Hard- und Softwareeinsatz

- **Beschaffung, Softwareentwicklung (M2.27)**
  Verantwortlich für Initiierung: HS-Leitung, SMT
  Verantwortlich für Umsetzung: IT-Verantwortliche, IT-Anwender/-innen

  Die Beschaffung von Soft- und Hardware ist mit dem zuständigen IT-Verantwortlichen und dem ZKI abzustimmen. Diese sind für die Einhaltung der IT-Konzeption der Hochschule, von Standards bzw. Sicherheitsanforderungen verantwortlich. Bei der Entwicklung von Software müssen vorher die fachlichen und technischen Anforderungen spezifiziert sein. Diese Arbeiten werden in enger Abstimmung mit den betroffenen Organisationseinheiten durchgeführt.

- **Kontrollierter Softwareeinsatz (M2.28)**
  Verantwortlich für Initiierung: IT-Verantwortliche; IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: ZKI, IT-Personal

  (Siehe auch Abschnitt Kontrollierter Softwareeinsatz (M 1.7))

  Bei der Freigabe von Software muss darauf geachtet werden, dass die Software aus zuverlässiger Quelle stammt und dass ihr Einsatz notwendig ist.

- **Separate Entwicklungsumgebung (M2.29)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Verantwortliche, IT-Personal

  Die Entwicklung oder Anpassung, insbesondere von serverbasierter Software, darf nicht in der Produktionsumgebung erfolgen. Die Überführung der Software von der Entwicklung in den Produktionsbetrieb bedarf der Freigabe durch den zuständigen IT-Verantwortlichen.

- **Test von Software (M2.30)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal

  Vor dem Einsatz neuer Hardware-Komponenten oder neuer Software/ Versionen müssen diese auf speziellen Testsystemen hinreichend geprüft werden. Neben der Lauffähigkeit des Produktes ist dabei insbesondere zu überprüfen, dass der Einsatz neuer Komponenten keine negativen Auswirkungen auf die laufenden IT-Systeme hat. Da vor erfolgreichen Tests Schadfunktionen nicht ausgeschlossen werden können und da bei Tests Fehler provoziert werden, sind immer vom Produktionsbetrieb isolierte Testsysteme zu verwenden. Der Testverlauf und das Testergebnis sind zu dokumentieren. Erst nach bestandenem Test dürfen neue Komponenten für die Installation auf Produktionssystemen freigegeben werden.

- **Zeitnahes Einspielen sicherheitsrelevanter Patches und Upgrades (M2.31)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Um entdeckte Schwachstellen in Software-Produkten und bestimmten Hardware-Komponenten schnellst möglich zu beheben, damit sie nicht durch potentielle Angreifer ausgenutzt werden können ist es unabdingbar, dass Patches und Updates der Hersteller zeitnah eingespielt werden. Neben dem Betriebssystem sind auch die eingesetzten Applikationen (einschließlich ihrer Erweiterungen) und Treiber stets aktuell zu halten. Die Software sollte durch automatische Update-Services oder den regelmäßigen Besuch der Hersteller-Webseiten immer auf dem aktuellen Stand gehalten werden. Systemadministratoren/rinnen sollten sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren. Die Integrität und Authentizität der einzuspielenden Sicherheitsupdates und Patches ist sicherzustellen (Nutzung vertrauenswürdigen Quellen), außerdem sind sie immer mit Hilfe eines Malwareschutzprogramms zu prüfen.

- **Schutz vor Schadprogrammen (M2.32)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal

  (Siehe auch Abschnitt Malwareschutz (M 1.8))

  Das IT-Personal hat im eigenen Verantwortungsbereich dafür Sorge zu tragen, dass die im Abschnitt (M 1.8) beschriebenen Maßnahmen umgesetzt werden.

  Sollte durch Nutzer der Verdacht des Malwarebefalls gemeldet werden, sind durch eine/n Administrator/in die betroffenen Systeme zu ermitteln, weitere Ausbreitung zu verhindern und die Systeme in einen betriebsbereiten Zustand zurück zu versetzen. Nachdem alle Schadprogramme entfernt worden sind, müssen alle von diesem Rechner aus genutzten Zugangskennungen und Passwörter geändert werden, um einem möglichen Missbrauch vorzubeugen.

- **Kontrollierte PC-Schnittstellen (M2.33)**
  Verantwortlich für Initiierung: IT-Verantwortliche
  Verantwortlich für Umsetzung: IT-Personal

  Bei erhöhtem Schutzbedarf müssen Rechner so konfiguriert bzw. abgesichert werden, dass die Nutzung aller Schnittstellen des PCs (zum Beispiel DVD-Laufwerke, WLAN-Schnittstellen, USB-Ports oder interne Festplattenanschlüsse) ausgeschlossen wird, wenn sie für die zu erledigenden Aufgaben nicht notwendig sind. Für den Betrieb notwendige Schnittstellen müssen so kontrolliert werden, dass keine anderen als die vorgesehenen Geräte angeschlossen werden können. (Beispielsweise muss der USB-Port für den Anschluss einer Tastatur so eingestellt und überwacht werden, dass kein anderes Gerät an diesem Anschluss betrieben werden kann.) Der Zugriff auf das BIOS ist durch ein Passwort zu schützen.

- **Dokumentation (M2.34)**
  Verantwortlich für Initiierung: IT-Verantwortliche, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal

  Zu jedem IT-System soll eine Dokumentation geführt werden. Üblicherweise werden nicht einzelne PCs gesondert dokumentiert, sondern zu größeren Gruppen zusammengefasst. Die Dokumentation soll mindestens den Aufstellungsort und Unterlagen zur Hard- und Softwareausstattung, Garantieleistungen, Wartungsverträgen, Lizenzen usw. enthalten. Darüber hinaus sollten Angaben zur Hard- und Softwarekonfiguration, zu durchgeführten Reparaturarbeiten, aufgetretenen Problemen, Suche nach Schadprogrammen und zur Verantwortlichkeit dokumentiert werden. Regelungen zur Datensicherung (Umfang, Verfahren, Rhythmus usw.) sollen auch dokumentiert werden. Gut und aktuell dokumentierte IT-Systeme erleichtern Administrationsarbeiten, die Planung und Neuinstallation von Software, ebenso wie die Fehlerbeseitigung.

- **Ausfallsicherheit (M2.35)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: ZKI, IT-Personal

  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) oder Wartungsverträge mit kurzen Reaktionszeiten hinreichend verfügbar gehalten werden.

- **Einsatz von mobilen IT-Geräten (M2.36)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal

  Mobile IT-Geräte (z.B. Notebooks, PDA, Smartphone) können typischerweise sowohl mobil als auch stationär genutzt werden und damit auch auf unterschiedliche Netze zugreifen. Daraus resultiert, dass bei der mobilen Nutzung die Daten auf dem mobilen PC gegen Verlust, Manipulation und unberechtigte Einsichtnahme geschützt werden müssen. Andererseits muss sichergestellt werden, dass keine Gefährdungen von mobilen PCs auf andere IT-Systeme und Netze ausgehen können. Es ist unbedingt zu vermeiden, dass bei mobilen IT-Geräten mehrere Netzwerkschnittstellen gleichzeitig aktiviert sind. Bei der Nutzung von mobilen PCs durch verschiedene Personen muss die Übergabe geregelt stattfinden. Dabei muss mindestens nachvollziehbar sein, wo sich das Gerät befindet und welche Person das Gerät benutzt.

- **Einsatz von Diebstahl-Sicherungen (M2.37)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, Dezernat IV

  Mechanische oder elektronische Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen – z.B. geeignete Zutrittskontrolle zu den Arbeitsplätzen – nicht umgesetzt werden können, wie etwa bei Laptops im mobilen Einsatz.

  Diebstahl-Sicherungen sind z.B. dort sinnvoll, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Mit Diebstahl-Sicherungen sollten je nach zu schützendem Objekt nicht nur das IT-System selber, sondern auch Monitor, Tastatur und anderes Zubehör ausgestattet werden.

3.2.6. Zugriffsschutz

Grundsätzlich gilt, dass nur die Personen Zugang zum Netz und den damit verfügbaren Ressourcen der Hochschule Magdeburg-Stendal erhalten, die zuvor die Erlaubnis zur Nutzung von den dafür zuständigen Stellen erhalten haben. Jede Nutzungserlaubnis muss personengebunden sein, d.h. anonyme Nutzerkonten sollten nur in begründeten Ausnahmefällen (beispielsweise als Zugang für FTP- oder WWW-Server) erlaubt werden. Die Verwendung fremder Nutzerkennungen ist nicht erlaubt. In der Regel ist der Zugang zum Netz verbunden mit dem Zugriff auf Daten, Anwendungsprogramme und weitere Ressourcen. Daher hat die Authentisierung der Nutzer des Netzes an jedem einzelnen Arbeitsplatz-PC der Hochschule eine besondere Bedeutung.

- **Bereitstellung von Verschlüsselungssystemen (M2.38)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: ZKI, IT-Personal

  Zur Absicherung besonders schützenswerter Daten, insbesondere auf mobilen Computern, müssen geeignete Systeme (Programme oder spezielle Hardware) zur Verschlüsselung verwendet werden.

- **Netzzugänge (M2.39)**
  Verantwortlich für Initiierung: IT-Sicherheitsmanagement-SMT
  Verantwortlich für Umsetzung: ZKI, IT-Verantwortliche, IT-Sicherheitsbeauftragte

  Der Anschluss von Systemen an das Datennetz der Hochschule Magdeburg-Stendal hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (WLAN-Accesspoints, Modems, Bridges, o.ä.) ohne Absprache mit dem ZKI und dem/der IT-Verantwortlichen der Organisationseinheit ist unzulässig.

- **Personenbezogene Kennungen (Authentisierung) (M2.40)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal

  Alle IT-Systeme und Anwendungen sind so einzurichten, dass nur berechtigte Benutzer/innen die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist eine Anmeldung mit Benutzerkennung und Passwort 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/Der Benutzer/in ist untersagt, Kennungen und Passwörter weiter zu geben. Die Zuordnung von mehreren Kennungen zu einer Person innerhalb eines IT-Systems sollte nur in begründeten Ausnahmefällen erlaubt sein, wie beispielsweise für Systemadministratoren. Die Einrichtung und Freigabe einer Benutzerkennung dürfen nur in einem bereichsintern geregelten Verfahren erfolgen und sind zu dokumentieren.

- **Administratorkennungen (M2.41)**
  Verantwortlich für Initiierung: IT-Verantwortliche, IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal

  Das Verwenden von Benutzerkennungen mit Administrationsrechten muss auf die dafür notwendigen Aufgaben beschränkt bleiben. Die Administratoren/innen erhalten für diese Aufgaben eine persönliche Administratorkennung. Für die alltägliche Arbeit sind Benutzerkennungen mit eingeschränkten Rechten zu verwenden. Administrator-Konten sind möglichst umzubenennen, damit deren Bedeutung nicht sofort ersichtlich ist.

- **Ausscheiden von Mitarbeitern/-innen (M2.42)**
  Verantwortlich für Initiierung: Bereichsleitung
  Verantwortlich für Umsetzung: Vorgesetzte/r des betreffenden Mitarbeiters/-in

  Der/Die zuständige IT-Verantwortliche bzw. Verfahrensverantwortliche muss rechtzeitig über das Ausscheiden oder den Wechsel eines/r Mitarbeiters/in informiert werden. Die zuständige Organisationseinheit der/des Betreffenden hat über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung des/der ausscheidenden Mitarbeiters/in zugeordnet sind. Vor dem Ausscheiden sind sämtliche Unterlagen, die sicherheitsrelevante Angaben enthalten sowie ausgehändigte Schlüssel zurück zu fordern. Es sind ihr/ihm sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. 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.

  Die Weiterführung der übertragenen sicherheitsrelevanten Aufgaben und Funktionen muss auch nach dem Ausscheiden weiter gewährleistet bleiben. Vor dem Weggang ist eine rechtzeitige Einweisung des/der Nachfolgers/in durchzuführen. Dafür ist es wünschenswert, dass sich die Arbeitszeiträume wenigstens kurz überschneiden. Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen.

Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren. Die bestehenden Vertretungsregelungen sind ebenfalls zu überprüfen und ggf. zu aktualisieren.

- **Gebrauch von Passwörter (M2.43)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal IT-Anwender/-innen

  Werden in einem IT-System Passwörter zur Authentisierung gebraucht, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gebraucht wird. Der/Die Benutzer/in hat sein/ihr Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden. Für die Wahl von Passwörtern werden folgende Regeln dringend empfohlen:

  1. Das Passwort darf nicht leicht zu erraten sein, wie Namen, Geburtsdatum.
  2. Das Passwort muss mindestens einen Buchstaben und mindestens eine Ziffer oder ein Sonderzeichen enthalten.
  3. Das Passwort sollte mindestens 8 Zeichen lang sein.
  4. Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
  5. Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
  6. Das Passwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt werden soll. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.
  7. Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.
  8. Die Eingabe des Passwortes muss unbeobachtet stattfinden.

  Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:

  1. Jede/r Benutzer/in muss sein/ihr eigenes Passwort jederzeit ändern können.
  2. Bei der Authentisierung in vernetzten Systemen sollten Passwörter nicht unverschlüsselt übertragen werden.

- **Zugriffsrechte (Autorisierung) (M2.44)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte,
  Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Verantwortliche, IT-Personal

  (Siehe auch Abschnitt Zugriffsrechte (M 1.12))

  Bei der Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer/innen sind die in den Bereichen geltenden besonderen Regelungen zu beachten.

  Zugriffsrechte sind restriktiv zu vergeben. Für Benutzer mit besonderen Rechten, insbesondere für Administratorkennungen, ist eine Zugangsbegrenzung auf die notwendigen Rechner (i.d.R. sind es der betreffende Server und die Arbeitsplatz-PCs) zu begrenzen. Es ist ebenfalls zu prüfen, inwieweit die Zugangserlaubnis auf bestimmte Zeiten begrenzt werden kann (Arbeitszeit).

Das zuständige IT-Personal muss über die notwendige Änderung der Berechtigungen eines Anwenders, z. B. in Folge von Änderungen seiner Aufgaben, rechtzeitig informiert werden, um die Berechtigungsänderungen im System abzubilden. Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren.

- **Abmelden und ausschalten (M2.45)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Soweit es technisch möglich ist, sind zentral administrierte IT-Systeme so zu konfigurieren, dass die Maßnahmen im Abschnitt Abmelden und ausschalten (siehe M 1.9), umgesetzt werden und durch den/die Benutzer/in nicht ohne weiteres deaktiviert werden können.

3.2.7. System- und Netzwerkmanagement

Eine angemessene Protokollierung, Audit und Revision sind wesentliche Faktoren der Netzsicherheit. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt, oder die Erkennung von systematischen Angriffen auf das Netz. Unter einem Audit wird die Verwendung eines Dienstes verstanden, der insbesondere sicherheitskritische Ereignisse betrachtet. Bei einem Audit werden die Ereignisse mit Hilfe geeigneter Werkzeuge betrachtet und ausgewertet. Protokolle dienen 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 (DSG LSA). Je nach Schutzbedarf des Verfahrens müssen adäquate Maßnahmen zur Protokollierung getroffen werden, um die Revisionsfähigkeit zu gewährleisten.

- **Protokollierung (M2.46)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte, Verfahrensverantwortliche
  Verantwortlich für Umsetzung: ZKI, IT-Verantwortliche, Datenschutz

  Je nach den Möglichkeiten des Betriebssystems sind alle Zugangsversuche zu schützenswerten IT-Systemen, sowohl die erfolgreichen als auch die erfolglosen, automatisch zu protokollieren. Das Ändern wichtiger Systemparameter und auch das Herunterfahren bzw. das Hochfahren dieser Systems sollten ebenfalls automatisiert protokolliert werden.

  In Protokolldateien, die personenbezogene Daten beinhalten, ist das Prinzip der Zweckbindung gemäß DSG LSA unbedingt einzuhalten.

3.2.8. Kommunikationssicherheit

Die gesamte elektronische Kommunikation der Hochschule wird durch eine Sicherheitsinfrastruktur in angemessener Weise geschützt. Besonderes Augenmerk gilt dabei der Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf. Alle IT-Nutzer der Hochschule sind über die besonderen Risiken und Gefahren der elektronischen Kommunikation und der Datenübermittlung in Kenntnis zu setzen.

- **Sichere Netzwerkadministration (M2.47)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: ZKI, IT-Verantwortliche, IT-Personal

  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. Die Netzdokumentation ist verschlossen zu halten und vor dem Zugriff Unbefugter zu schützen.

- **Netzmonitoring (M2.48)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
  Verantwortlich für Umsetzung: IT-Verantwortliche, IT-Personal

  Es müssen geeignete Maßnahmen getroffen werden, um 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.

- **Deaktivierung nicht benötigter Netzwerkzugänge (M2.49)**
  Verantwortlich für Initiierung: SMT, IT-Verantwortliche
  Verantwortlich für Umsetzung: ZKI

  Es sind alle nicht benötigten Netzwerkzugänge zu deaktivieren, damit ein unbefugter Zugang zum Netz der Hochschule Magdeburg-Stendal verhindert wird.

- **Kommunikation zwischen unterschiedlichen Sicherheitsniveaus (M2.50)**
  Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter
  Verantwortlich für Umsetzung: ZKI

  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 (z.B. zu Fernwartungszwecken), muss dies zuvor durch die zuständige Stelle genehmigt werden. Zu diesem Zweck kann durch das ZKI ein administrativer VPN-Zugang angelegt werden. Jeder Zugriff Externer ist zu protokollieren.

3.2.9. Datensicherung

- **Organisation der Datensicherung (M2.51)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: ZKI, IT-Personal

  Die Datensicherung muss nach einem dokumentierten Datensicherungskonzept erfolgen, das dem Schutzbedarf der zu sichernden Daten angemessen ist. Es muss auch darüber Auskunft geben, nach welchen Kriterien die Sicherung der Daten erfolgt. Im Falle personenbezogener Daten sind die geforderten Mindest- bzw. Höchstzeiträume 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.

- **Durchführung der Datensicherung (M2.52)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: ZKI, IT-Personal, IT-Anwender/-innen

  Vorzugsweise sollen Daten auf zentralen Fileservern gespeichert werden. Von dort sollte turnusgemäß eine Sicherung auf dem zentralen Archiv-Backup-System (ZABS) der Hochschule erfolgen. Einzelheiten hierzu sind der Dienstbeschreibung des ZABS (http://www.zki.hs-magdeburg.de/dienste/tsm) zu entnehmen. Datenbestände ab Schutzklasse „hoch“ sind auf jeden Fall auf dem ZABS zu sichern. Wo ein Zugriff auf einen Fileserver oder das ZABS derzeit noch nicht möglich ist, müssen die Daten lokal gesichert werden. Es ist empfehlenswert, jeweils eine Sicherung für mindestens 3 bis 6 Monate aufzubewahren.

- **Durchführung der Datensicherung auf Servern (M2.53)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: ZKI, IT-Personal

  Die Sicherung der Daten auf Servern sollte im angemessenen Rhythmus erfolgen. Auch komplexe System- und Programmdaten sollten nach Veränderungen gesichert werden. Zur Datensicherung sind geeignete Backup-Werkzeuge zu verwenden. Für Daten, deren Wiederherstellung mehr als zwei Tage erfordert, sollte diese eine Sicherung nach dem Generationenprinzip unterstützen.

  Nach Möglichkeit sind die Konfigurationen aller aktiven Netzkomponenten in die regelmäßige Datensicherung zu involvieren.

3.2.10. Datenträgerkontrolle

- **Aufbewahrung (M2.54)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal

  Sicherungsdatenträger sind getrennt vom jeweiligen Rechner aufzubewahren. Bei längerer Lagerung sind Vorkehrungen zu treffen, die eine alterungsbedingte Zerstörung der Datenträger verhindern.

- **Weitergabe von Datenträgern und gesicherter Transport (M2.55)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal

  Die Weitergabe von Datenträgern darf nur an befugte Personen erfolgen. Befugt ist eine Person dann, wenn die Weitergabe der Datenträger im Verfahren vorgesehen ist. Die Übermittlung von Datenträgern mit vertraulichen Daten hat persönlich, per Kurier, per Wertbrief oder mit vergleichbaren Transportdiensten zu erfolgen.

- **Physisches Löschen und Entsorgung von Datenträgern (M2.56)**
  Verantwortlich für Initiierung: Verfahrensverantwortliche
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender/-innen

  Wenn Datenträger, auf denen schützenswerte Daten gespeichert sind, zur weiteren Verwendung an Dritte gehen, müssen alle Daten vor der Weitergabe physisch gelöscht werden. Das muss mit geeigneten Programmen erfolgen, die von den Betriebssystemen dafür vorgesehenen Programme genügen in der Regel nicht. Eine Weitergabe an hochschulfremde Personen ist untersagt. Auszusondernde oder defekte Datenträger müssen, sofern sie personenbezogene oder vertrauliche Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden.