Freie Universität Berlin

IT-Sicherheitsrichtlinie

der

Freien Universität Berlin

Version 4.0

04. April 2019

Steckbrief

Zielsetzung	Einheitliche Sicherheitsstandards zur Gewährleistung eines ordnungsgemäßen IT-Betriebs
Inhalt	Regelungen zur Informationssicherheit und Datenschutz
Zielgruppe	Alle Mitglieder der Freien Universität Berlin und Nutzer/innen deren IT-Ressourcen
Geltungsbereich	Alle Einrichtungen der Freien Universität Berlin
Gültigkeitsdauer	Unbegrenzt

Autoren

Hr. Camphausen
Hr. Dräger
Hr. Dr. Haase
Fr. Heinau
Hr. Posel
Hr. Dr. Sommerer
Hr. Tietz
Fr. Dr. Wittkopf
Hr. Worch

Inhaltsverzeichnis

Verzeichnis der IT-Grundschutzmaßnahmen

Präambel

Um das Ziel „ausreichende und angemessene IT-Sicherheit[1)]“ in der Freien Universität Berlin zu erreichen, wurden die Empfehlungen und Vorschläge des Bundesamts für Sicherheit in der Informationstechnik (BSI) zugrunde gelegt und an die Bedürfnisse der Freien Universität Berlin 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 und vollständigen Ergebnis führt. Voraussetzung dafür ist die konstruktive Zusammenarbeit aller Beteiligten.

In der IT-Sicherheitsrichtlinie werden wesentliche Aspekte des Datenschutzes berücksichtigt. Insbesondere genügen die Regelungen dieser Richtlinie den datenschutzrechtlichen Ansprüchen an eine Dokumentation der Verarbeitungsprozesse. 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 von der Arbeitsgruppe IT-Sicherheit mit der Absicht entwickelt, um allen Mitarbeiterinnen und Mitarbeitern eine Handreichung zu bieten, die notwendigen und angemessenen Sicherheitsvorkehrungen bei der Planung und dem Betrieb von Informationstechnik auszuwählen.

Kurzbeschreibung

Die IT-Sicherheitsrichtlinie der Freien Universität Berlin ist das zentrale Regelwerk für alle Themenbereiche der IT-Sicherheit und enthält auch Präzisierungen der datenschutzrechtlichen Anforderungen. Neben verschiedenen Schutzmaßnahmen werden die Erfassung, Bewertung und Dokumentation von IT und der datenverarbeitenden Prozesse detailliert vorgegeben.

Die Richtlinie ist in vier Hauptteile untergliedert. Im ersten Teil werden Begriffsdefinitionen vorgenommen und wesentliche organisatorische Strukturen festgelegt. Der zweite Teil beschreibt die Dokumentation des IT-Einsatzes und der Datenverarbeitung. Insbesondere wird in diesem Teil die Methode zur Ermittlung der Sensibilität der verarbeiteten Daten und der Risikoanalyse festgelegt. Der dritte Teil enthält eine Sammlung von technisch-organisatorischen Grundschutzmaßnahmen, die in jedem Fall umgesetzt werden müssen. Im vierten und letzten Teil wird der Umgang mit bzw. die Anwendung dieser Richtlinie erklärt.

[1)] IT = Informationstechnik

Teil I Allgemeines

Die Freie Universität Berlin setzt in hohem Maße Informationstechnologie in ihren Kernprozessen ein:

- Forschung: Zum Beispiel weltweite Kommunikation und Zusammenarbeit, digitale Publikation und Recherche, rechenintensive Anwendungen, IT-gestützte Messverfahren
- Lehre: Zum Beispiel e-Learning, digitale Bibliothekssysteme, das elektronische Management von Lehrveranstaltungen
- Verwaltung: Zum Beispiel Verwaltung von Personal-, Studierenden- und Prüfungsdaten, Finanzsteuerung

Verbunden mit dem zunehmenden IT-Einsatz an der Freien Universität Berlin steigt auch die Abhängigkeit der Universität 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)
- Selbstverpflichtung: Zum Beispiel des Ehrenkodexes der Freien Universität Berlin (wissenschaftliche Primärdaten müssen 10 Jahre aufbewahrt werden)

Es sind daher Maßnahmen zu treffen, die die Funktionsfähigkeit der Freien Universität Berlin 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 Freien Universität 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 sicherheitstechnischen und datenschutzrechtlichen Betrachtung. Die Dokumentationspflicht wird an der Freien Universität durch die Beschreibung von IT-Verfahren erfüllt.

Der für jeden IT-Arbeitsplatz zu erreichende Grundschutz bildet das Fundament der IT-Sicherheit der Freien Universität Berlin. 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 Freien Universität Berlin verbindlich. Die IT-Sicherheitsrichtlinie gilt darüber hinaus auch für alle externen Nutzer/innen der IT-Infrastruktur der Freien Universität Berlin.

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

Alle Nutzer/innen von IT-Ressourcen der Freien Universität Berlin werden über die für sie relevanten Teile der IT-Sicherheitsrichtlinie informiert. Neue Mitglieder der Freien Universität Berlin werden auf die geltende IT-Sicherheitsrichtlinie beim Eintritt in die Freie Universität hingewiesen. Nicht-Mitglieder, die IT-Ressourcen der Freien Universität Berlin 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 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 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 Freien Universität 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 Freien Universität für den IT-Einsatz festgelegten Rollen und Zuständigkeiten sind in der IT-Organisationsrichtlinie der Freien Universität Berlin beschrieben. Die für die IT-Sicherheit aus organisatorischer und strategischer Sicht bedeutendsten Rollen werden an dieser Stelle kurz dargestellt:

- **Höchste Entscheidungsinstanz (Präsident)**
  Die höchste Entscheidungsinstanz und Träger der Gesamtverantwortung an der Freien Universität in allen IT-Fragen ist der Präsident der Freien Universität Berlin.
- **Strategische und operative Führung des IT-Einsatzes (CIO)**
  Im Auftrag des Präsidiums ist der CIO (Chief Information Officer) für alle Aufgaben der strategischen Führung der Informationstechnologie und der bereichsübergreifenden operativen Vorgaben verantwortlich.
- **Bereitstellung von zentralen IT-Diensten (Zentrale IT-Servicebereiche)**
  Die zentralen IT-Servicebereiche (Zentraleinrichtung für Datenverarbeitung – ZEDAT, Universitätsbibliothek – UB, elektronische Administration und Services – eAS) planen, realisieren, betreiben und gestalten IT-Infrastrukturen und -Services für die Einrichtungen der Freien Universität Berlin.
- **Koordination und Organisation der Informationssicherheit (IT-Sicherheitsbeauftragter)**
  Die Aufgabe der Koordination und Organisation der Informationssicherheit obliegt dem IT-Sicherheitsbeauftragten der Freien Universität Berlin. Er ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Freien Universität Berlin.
- **Datenschutz (Der/die behördliche/r Datenschutzbeauftragter)**
  Dem behördlichen Datenschutzbeauftragten obliegt die Unterstützung des Präsidiums 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 Freien Universität Berlin und macht die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Erfordernissen des Datenschutzes vertraut.
- **Bereichsbezogener IT-Einsatz**
  - **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 IT-Beauftragten, der den IT-Einsatz koordiniert und plant und darüber hinaus die in der IT-Sicherheitsrichtlinie formulierten Maßnahmen umsetzt.
  - **IT-Sicherheitsbeauftragter**
    Der IT-Sicherheitsbeauftragte koordiniert und organisiert die Informationssicherheit. Er ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb des Bereichs.

  - **IT-Beauftragter**
    Der IT-Beauftragte bildet die Schnittstelle zwischen der von ihm vertretenden Einrichtung und anderen FU-Bereichen sowie der Universitätsleitung. Zum einen bündelt er die Anforderungen und den Bedarf an IT-Unterstützung seiner Einrichtung und kommuniziert diese an die universitären IT-Servicebereiche bzw. an die Universitätsleitung. Zum anderen informiert er die Beschäftigten der Einrichtung über zentrale Vorgaben und sorgt für deren Umsetzung in seiner Einrichtung. Die Rolle des IT-Beauftragten ist ausführlich in dem Handlungsleitfaden "Einbindung des IT-Beauftragten in wichtige Prozesse eines Fachbereichs"[2)] beschrieben.

- **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 Datenschutzes und der Informationssicherheit.

- **AG IT-Sicherheit**
  Die Arbeitsgruppe IT-Sicherheit berät zu allen Fragen der IT-Sicherheit und erstellt Empfehlungen für die Leitung der Freien Universität Berlin. 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 IT-Beauftragten untereinander und mit den universitären IT-Dienstleistern.

  Die Zusammensetzung der Arbeitsgruppe IT-Sicherheit berücksichtigt die Vielfalt der unterschiedlichen Anforderungen der Bereiche (Forschung und Lehre, Dienstleister, Verwaltung) an den IT-Einsatz.

Zusätzlich zu den oben beschriebenen Rollen gibt es im Kontext von IT-Verfahren weitere Rollen (siehe Abschnitt 5.4):

- Systemadministrator
- Applikationsbetreuer
- Key-User
- Anwender

4 Grundbegriffe

Im Folgenden werden die zentralen Begriffe der IT-Sicherheitsrichtlinie der Freien Universität Berlin erläutert.

- **Geschäftsprozess**
  Ein Geschäftsprozess ist eine Menge zusammenwirkender Einzeltätigkeiten (Aufgaben, Arbeitsabläufe), die ausgeführt werden, um ein bestimmtes geschäftliches Ziel zu erreichen.

[2)] Das genannte Regelwerk ist auf den Webseiten der AG IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 12 Literaturverzeichnis) abrufbar.

- **IT-Verfahren**
  Die Summe aller IT-Verfahren soll den gesamten IT-Einsatz an der Freien Universität 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, so lange 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 und aller Informationen der Freien Universität Berlin.

Teil II IT-Verfahren

5 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 6 dieser Richtlinie)

c) Risikoanalyse in Abhängigkeit vom Ergebnis der Schutzbedarfsanalyse (siehe Abschnitt 7 dieser Richtlinie)

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 Regelungen 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 erstellt 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 • verschiedene Datenkategorien • verschiedene „Datenbesitzer“	• Zusammenhängende Aufgaben • Praktikabilität • 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 zusammenhängenden Prozessen der Freien Universität. Unterschiedlicher Schutzbedarf der Daten, verschiedene Datengruppen sowie verschiedene Dateneigentümer legen eine Differenzierung in mehrere Geschäftsprozesse nahe.

5.1 IT-Verfahrensdatenbank

Für die Dokumentation von IT-Verfahren muss die von der Freien Universität 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 Freien Universität Berlin zur Kenntnis gegeben werden. Dort wird die weitere Vorgehensweise mit der/dem Verfahrensverantwortlichen abgestimmt.

5.2 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.

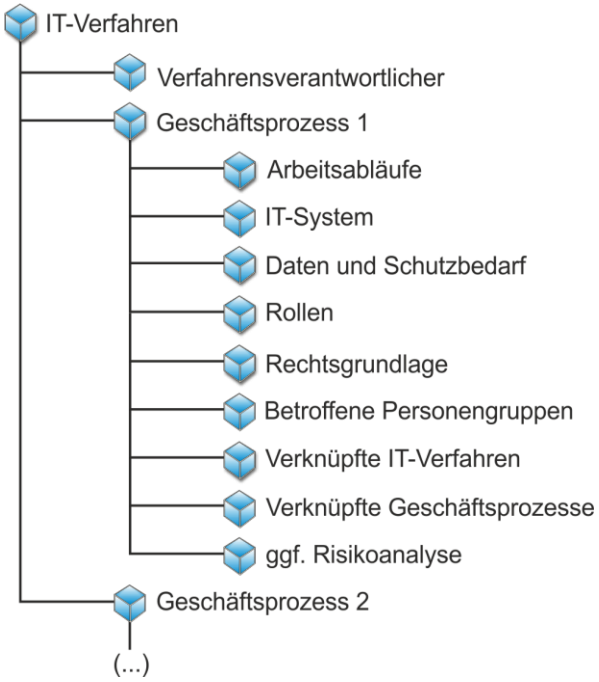

Abbildung 1: Vereinfachte Darstellung der typischen Komponenten eines IT-Verfahrens

5.3 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 ZEDAT den Dienst beschreibt.

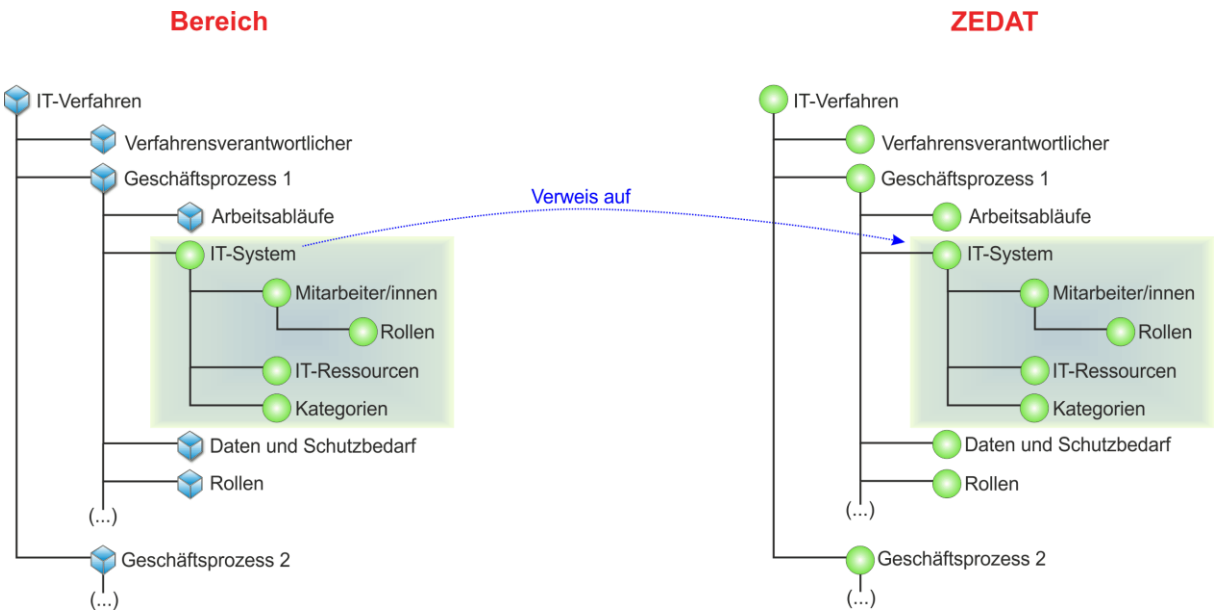

Abbildung 2: Beispiel: Ein IT-Verfahren in einem Fachbereich nutzt einen Dienst der ZEDAT.

5.4 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	Anmerkungen
Verfahrensverantwortliche/r	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 • zuständig für die Einhaltung des Betriebs- und Datensicherungskonzepts	obligatorisch für einen ordnungsgemäßen Betrieb

Rolle	Funktion	Anmerkungen
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: Übersicht der Rollen

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.

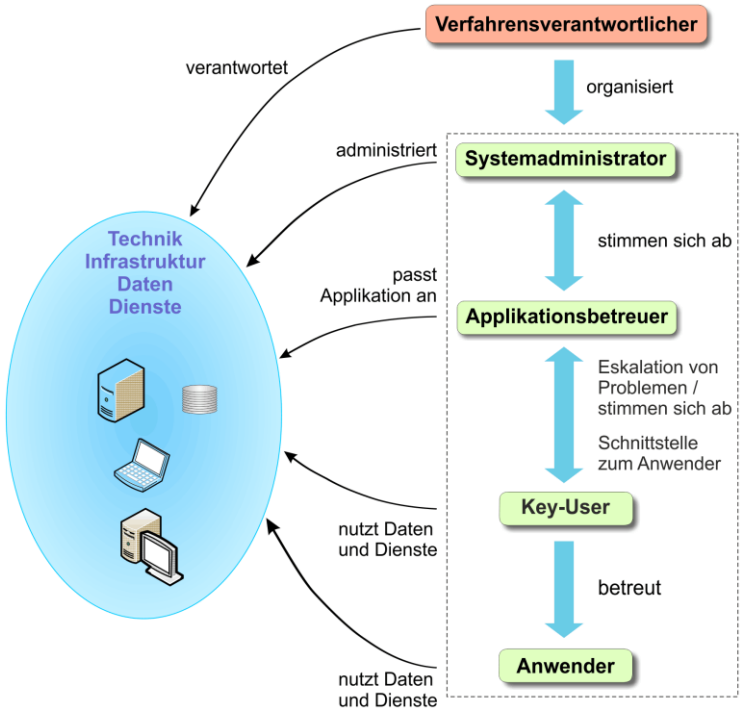

Abbildung 3: Zusammenwirken der Rollen

5.5 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 5.1 anzulegen und der Betrieb dem IT-Sicherheitsbeauftragten der Freien Universität Berlin anzuzeigen und die Sicherheit der betroffenen Systeme sowie der zugrundeliegenden Infrastruktur zu gewährleisten.

6 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 6.2 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 7 beschrieben.

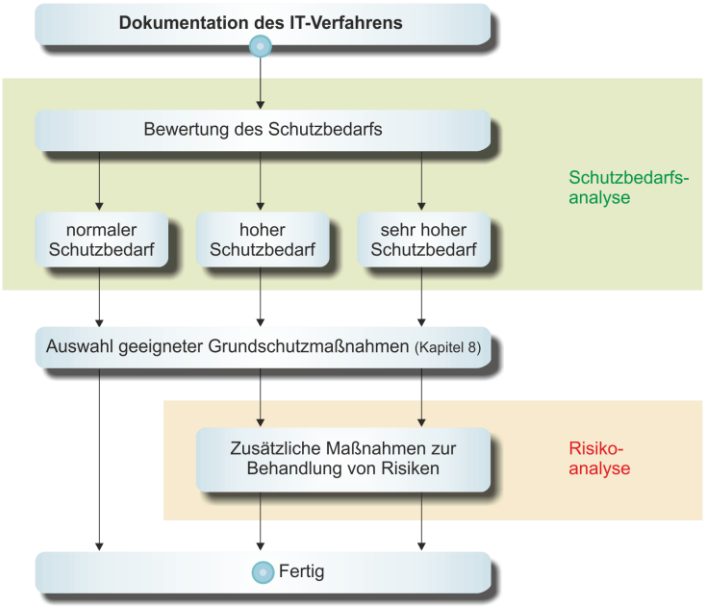

Abbildung 4: Vereinfachte Darstellung der analytischen Schutzbedarfsbewertung

6.1 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 6.2 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, Postleitzahl 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 Freie Universität Berlin 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 Auswirkungen 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 6.2) 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.

In diesem fiktiven Beispiel wurde ein IT-Verfahren betrachtet, in dem die negative Außenwirkung bezüglich der Vertraulichkeit hoch ist:

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

Tabelle 3: Beispiel für das Ergebnis einer Schutzbedarfsbetrachtung

6.2 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).

6.2.1 Verlust von Vertraulichkeit

Verlust von Vertraulichkeit				
Schadenskategorien	**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 Freien Universität gefährden. Kernprozesse der Universität können massiv behindert werden.
Negative Außenwirkung	Missbrauch der Daten führt zu:	• Geringer Ansehensverlust eines Teilbereichs der Freien Universität bei einer eingeschränkten Öffentlichkeit	• Ansehensverlust der gesamten Freien Universität bei einer eingeschränkten Öffentlichkeit • Hoher Ansehensverlust eines Teilbereichs der Freien Universität	• Ansehensverlust der gesamten Freien Universität 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

Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren:

Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“. Die in der Zeile „Finanzielle Auswirkungen“ angegebenen Beträge wurden in Abhängigkeit von der Höhe des Haushalts der Freien Universität Berlin festgelegt.

6.2.2 Verletzung von Integrität

Verletzung von Integrität				
Schadenskategorien	**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 Freien Universität gefährden. Kernprozesse der Universität können massiv behindert werden.
Negative Außenwirkung	Unberechtigte Veränderung der Daten führt zu:	• Geringer Ansehensverlust eines Teilbereichs der Freien Universität bei einer eingeschränkten Öffentlichkeit • Erheblicher Ansehensverlust eines Teilbereichs der Freien Universität bei einer sehr kleinen und unbedeutenden Öffentlichkeit	• Ansehensverlust der gesamten Freien Universität bei einer eingeschränkten Öffentlichkeit • Hoher Ansehensverlust eines Teilbereichs der Freien Universität	• Ansehensverlust der gesamten Freien Universität 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

Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren:

Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“. Die in der Zeile „Finanzielle Auswirkungen“ angegebenen Beträge wurden in Abhängigkeit von der Höhe des Haushalts der Freien Universität Berlin festgelegt.

6.2.3 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 von Verfügbarkeit				
Schadenskategorien	**Bedrohung**	**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 Freien Universität gefährden. Kernprozesse der Universität können massiv behindert werden.
Negative Außenwirkung	Beeinträchtigung der Daten ...	• Geringer Ansehensverlust eines Teilbereichs der Freien Universität bei einer eingeschränkten Öffentlichkeit • Erheblicher Ansehensverlust eines Teilbereichs der Freien Universität bei einer sehr kleinen und unbedeutenden Öffentlichkeit	• Ansehensverlust der gesamten Freien Universität bei einer eingeschränkten Öffentlichkeit • Hoher Ansehensverlust eines Teilbereichs der Freien Universität	• Ansehensverlust der gesamten Freien Universität 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

Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren:

Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“. Die in der Zeile „Finanzielle Auswirkungen“ angegebenen Beträge wurden in Abhängigkeit von der Höhe des Haushalts der Freien Universität Berlin festgelegt.

6.2.4 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

- Berliner Datenschutzgesetz (BlnDSG)
- Informationsverarbeitungsgesetz (IVG)
- Bundesdatenschutzgesetz (BDSG)

Hochschulgesetze bzw. -verordnungen, FU-Richtlinien, beispielsweise

- Berliner Hochschulgesetz (BerlHG)
- Studierendendatenverordnung (StudDatVO)
- Datenschutzsatzung der Freien Universität Berlin
- IT-Sicherheitsrichtlinie der Freien Universität Berlin

Vorschriften zur Mitbestimmung, beispielsweise

- Landespersonalvertretungsgesetz Berlin (LPersVG-Berlin)
- IT-Grundsatzdienstvereinbarung der Freien Universität Berlin

Verträge, beispielsweise

- Vertrag über die Zusammenarbeit mit einer externen Firma

Verstoß gegen Gesetze, Vorschriften und Verträge			
Bedrohung	**Abschätzung des Schadens**		
Bekannt werden der Daten für Unberechtigte ...	… verstößt gegen Gesetze oder Vorschriften mit geringen Konsequenzen. [3)]	… verstößt gegen Gesetze oder Vorschriften mit erheblichen Konsequenzen.[3)]	... verstößt gegen Gesetze oder Vorschriften mit schwerwiegenden rechtlichen Konsequenzen.[3)]
Unberechtigte Veränderung der Daten …	… hat geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen zur Folge.	… hat Vertragsverletzungen mit hohen Konventionalstrafen und / oder erheblichen Haftungsschäden zur Folge.	… hat Vertragsverletzungen zur Folge, deren Haftungsschäden für die Freie Universität sehr hoch sind.
Verlust der Daten …			
daraus resultierender Schutzbedarf:	**normal**	**hoch**	**sehr hoch**

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“.

Die Dokumentation der Schutzbedarfsanalyse besteht aus den Ergebnissen der Bewertungstabellen 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)] Zur Einschätzung der rechtlichen Konsequenzen kann das vom Gesetzgeber vorgesehene Strafmaß hilfreich sein.

7 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 werden 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 Freie Universität geltenden Sicherheitsanforderungen genügt.

7.1 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

In der Risikoanalyse werden die für IT-Verfahren benötigten Komponenten als Zielobjekte bezeichnet. Die Zielobjekte können in Kategorien geordnet werden.

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

7.2 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 Freie Universität Berlin 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 Freie Universität Berlin 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	Feuer		✘	✘
M30	Ungünstige klimatische Bedingungen		✘	✘
M29	Wasser		✘	✘
M19, M20	Verschmutzung, Staub, Korrosion		✘	✘
M27	Ausfall oder Störung der Stromversorgung		✘	✘
M22, M23, M24	Ausfall oder Störung von Kommunikationsnetzen			✘
M41	Ausfall oder Störung von Dienstleistern	✘	✘	✘
M25	Ausspähen von Informationen / Spionage	✘		
M41, M42, M46	Verlust von Geräten, Datenträgern und Dokumenten	✘		✘
	Fehlplanung oder fehlende Anpassung	✘	✘	✘
M48, M60	Offenlegung schützenswerter Informationen	✘		
M35	Informationen aus unzuverlässiger Quelle	✘	✘	✘
	Manipulation von Hard- und Software	✘	✘	✘
	Manipulation von Informationen		✘	✘
M8	Unbefugtes Eindringen in IT-Systeme	✘	✘	✘
M41	Ausfall von Geräten oder Systemen		✘	✘
M37	Fehlfunktion von Geräten oder Systemen	✘	✘	✘
M16	Ressourcenmangel		✘	✘
M37	Software-Schwachstellen oder -Fehler	✘	✘	✘
M3, M7	Verstoß gegen Gesetze oder Regelungen	✘	✘	
M4, M52, M57	Unberechtigte Nutzung oder Administration von Geräten und Systemen	✘	✘	✘
M18, M39	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	✘	✘	✘
M1a, M4, M52, M54, M56, M57	Missbrauch von Berechtigungen	✘	✘	✘
M16, M17	Personalausfall			✘
M53, M56, M59	Identitätsdiebstahl	✘	✘	✘
	Missbrauch personenbezogener Daten	✘		
M35, M38	Schadprogramme	✘	✘	✘
M8, M14, M61, M61a, M62, M64	Störung von Diensten (Denial of Service)			✘
	Sabotage	✘	✘	✘
M1a, M80	Social Engineering	✘	✘	
M19	Unbefugtes Eindringen in Räumlichkeiten	✘	✘	✘
M68, M69, M70, M71	Datenverlust			✘
M71, M72	Integritätsverlust schützenswerter Informationen		✘	

Tabelle 12: Übersicht über die elementaren Gefährdungen mit den jeweils betroffenen Grundwerten

[4)] In dieser Spalte wird auf IT-Grundschutzmaßnahmen aus Teil III dieser Richtlinie verwiesen.

7.3 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.

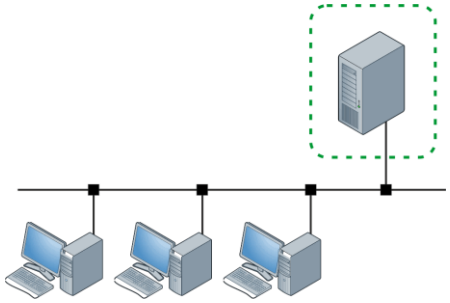

Abbildung 5: Fileserver in einer Netzwerkumgebung.

Ausgangssituation: Die Schutzbedarfsanalyse hat ergeben, dass die auf dem Fileserver abgelegten 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 sowie 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.

Tabelle 13: Identifizierung der beteiligten Komponenten

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

Tabelle 14: Auswahl der relevanten Objekte

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 angeschlossenen Client-Geräte sind für den Serverbetrieb nicht relevant.

Schritt 3: Bestimmung der Gefährdungen der ermittelten Komponenten.

Nr.	Zielobjekte	Gefährdung
1.	Fileserver	Unerlaubter Zugriff
2.	Netzwerk	Abhören
3.	Administratoren	Ausspähen
4.	Räume	Unerlaubter Zutritt
5.	Anwendung (Software)	Unerlaubter Zugang

Tabelle 15: Zusammenstellung der Gefährdungen der ermittelten Zielobjekte.

5) Es werden nur Komponenten ausgewählt, die eine potentielle Schwachstelle für Gefährdungen hinsichtlich des Verlusts der Vertraulichkeit darstellen können.

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.	Zielobjekte	Gefährdung	Häufigkeit[6)]
1.	Fileserver	Unerlaubter Zugriff	häufig
2.	Netzwerk	Abhören	selten
3.	Administratoren	Ausspähen	selten
4.	Räume	Unerlaubter Zutritt	selten
5.	Anwendung (Software)	Unerlaubter Zugang	mittel

Tabelle 16: Zusammenstellung der Eintrittswahrscheinlichkeit der Gefährdungen.

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

Nr.	Zielobjekte	Gefährdung	Häufigkeit	Schadens-höhe[7)]	Risiko[8)]
1.	Fileserver	Unerlaubter Zugriff	häufig	hoch	untragbar
2.	Netzwerk	Abhören	selten	hoch	tragbar
3.	Administratoren	Ausspähen	selten	hoch	tragbar
4.	Räume	Unerlaubter Zutritt	selten	hoch	tragbar
5.	Anwendung (Software)	Unerlaubter Zugang	mittel	hoch	tragbar

Tabelle 17: Bewertung der Risiken.

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 Freie Universität geltenden Sicherheitsanforderungen genügt.

---

6) Die Häufigkeit wird gemäß Tabelle 9 ermittelt.
7) Die Schadenshöhe ist das Ergebnis der Schutzbedarfsanalyse.
8) Das Risiko wird gemäß Tabelle 10 ermittelt.

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.	Zielobjekte	Gefährdung	Häufigkeit	Schadens-höhe	Risiko	Maß-nahme
1.	Fileserver	Unerlaubter Zugriff	häufig	hoch	untragbar	Maß-nahme 1
2.	Netzwerk	Abhören	selten	hoch	tragbar	–
3.	Administratoren	Ausspähen	selten	hoch	tragbar	–
4.	Räume	Unerlaubter Zutritt	selten	hoch	tragbar	–
5.	Anwendung (Software)	Unerlaubter Zugang	mittel	hoch	tragbar	–

Tabelle 18: Ergebnistabelle

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 Betrieb 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.

Teil III Regeln

8 Maßnahmen des IT-Grundschutzes

Die in diesem Abschnitt zusammengestellten Maßnahmen bilden die Basis für die IT-Sicherheit an der Freien Universität Berlin. 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 in Kapitel 7 beschriebenen Risikoanalysen 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 Freien Universität Berlin, allerdings werden beispielsweise auch Gastwissenschaftler/innen dazu gezählt, wenn sie im Rahmen ihres Aufenthalts an der Freien Universität Berlin IT-Ressourcen administrieren, warten oder betreuen.

Für alle Maßnahmen gilt, dass die Umsetzung von jeder Person eingefordert werden kann, die deren Notwendigkeit in einem konkreten Fall erkennt. Dies kann durch eine Information der zuständigen Stelle oder durch eine entsprechende Anordnung erfolgen.

Ausnahmen von den Maßnahmen müssen explizit festgelegt, genehmigt, zeitlich limitiert und dokumentiert werden. Als Genehmigungsinstanz fungiert der IT-Sicherheitsbeauftragte der Freien Universität.

8.1 Allgemeines

(M1) Grundsätze für den IT-Einsatz

Verantwortlich für Umsetzung: Präsidium

Beschaffung, Entwicklung und Einsatz von IT-Anwendungen und -Systemen, sowie die Verarbeitung von Daten haben sich nach den an der Freien Universität Berlin 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 Universitätsverwaltung.

(M1a) Schulungsangebot zu IT-Sicherheit und Datenschutz

Verantwortlich für Umsetzung: Präsidium

Im Rahmen des Weiterbildungsangebots für Beschäftigte der Freien Universität Berlin stellt die Hochschulleitung Schulungsangebote zu IT-Sicherheit und Datenschutz bereit. Ziel der Schulungsangebote ist es, die Nutzenden der Informationstechnik zu befähigen, spezifische Gefahren zu erkennen und angemessen reagieren zu können.

(M2) Verantwortung

Entfällt (integriert in M1).

8.2 Organisation von IT

(M3) 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 IT-Beauftragte informiert die Verfahrensverantwortlichen in seinem/ihrem Zuständigkeitsbereich über ihre Dokumentationspflichten.

(M4) 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.

(M5) Benennung einer/eines IT-Beauftragten

Verantwortlich für Umsetzung: Bereichsleitung

Jeder Bereich muss eine/n IT-Beauftragte/n und eine Abwesenheitsvertretung benennen. IT-Beauftragten kommt im Rahmen des IT-Einsatzes an der Freien Universität 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 die IT-Servicebereiche der Freien Universität bzw. an das Präsidium. Außerdem informieren sie die Beschäftigten der Einrichtung über zentrale Vorgaben und sorgen für deren Umsetzung in ihrer Einrichtung. Die wesentlichen Aufgaben der IT-Beauftragten sind in dem Handlungsleitfaden „Einbindung des IT-Beauftragten in wichtige Prozesse eines Fachbereichs“ beschrieben.
Das genannte Regelwerk ist auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

(M6) Einbindung der IT-Beauftragten in Entscheidungsprozesse

Verantwortlich für Umsetzung: Bereichsleitung

Damit die/der IT-Beauftragte ihre/seine Aufgaben effizient wahrnehmen kann, sollte die Stelle des IT-Beauftragten organisatorisch der Bereichsleitung direkt unterstellt sein.

Sie/Er ist in alle Entscheidungsfindungsprozesse mit IT-Relevanz einzubeziehen. Insbesondere muss die/der IT-Beauftragte bei allen IT-Beschaffungsmaßnahmen, bei baulichen Maßnahmen und Umzügen sowie bei den IT-bezogenen Phasen eines Berufungsverfahrens beteiligt werden. Darüber hinaus muss die Bereichsleitung sicherstellen, dass die/der IT-Beauftragte über alle IT-relevanten Vorhaben und Planungen des Bereichs frühzeitig Kenntnis erhält. Weitere Einzelheiten können dem Handlungsleitfaden „Einbindung des IT-Beauftragten in wichtige Prozesse eines Fachbereichs“ entnommen werden.
Das genannte Regelwerk ist auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

(M7) Dokumentation der IT-Verfahren

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r

IT-Verfahren sind gemäß den in Abschnitt 5 formulierten Anforderungen zu dokumentieren. Nur dokumentierte Verfahren dürfen betrieben werden. Die/Der IT-Beauftragte 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 Applikationsbetreuer sind dabei durch die IT-Organisationsrichtlinie zur Mitarbeit verpflichtet.

(M8) 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:

- Zuständige/r IT-Beauftragte/r
- Zuständige IT-Abteilung bzw. IT-Gruppe
- Info-Service IT

Je nach dem wo der Vorfall gemeldet wird, erfolgt eine erste Bewertung durch die/den IT-Beauftragte/n, die IT-Abteilung des betroffenen Bereichs oder durch den Info-Service IT[9)]. Hier wird über die weiteren Bearbeitungsschritte und über die Information und Einbeziehung weiterer Stellen entschieden. Gegebenenfalls wird gemäß dem Handlungsleitfaden zur Behandlung von IT-Sicherheitsvorfällen weiter vorgegangen.

Jeder Sicherheitsvorfall muss durch die bearbeitende Stelle dokumentiert werden.

[9)] Annahmestelle für Support-Anfragen des Hochschulrechenzentrums.

(M9) Regelungen der Datenverarbeitung im Auftrag

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r

Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag der Freien Universität Berlin 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 des Berliner Datenschutzgesetzes (§ 48 BlnDSG) zu beachten. Darüber hinaus sind die Empfehlungen und Hinweise des Handlungsleitfadens „Zugriff auf schützenswerte Daten der Freien Universität Berlin durch Externe“ zu beachten.

Der genannte Leitfaden ist auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

(M10) 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 CIO definierten Strategien zu formulieren und regelmäßig neuen Anforderungen anzupassen. Bei der Entwicklung der Standards sind die spezifischen Bedürfnisse der Fachbereiche zu berücksichtigen.

(M11) Zentralisierung wichtiger Serviceleistungen

Verantwortlich für Umsetzung: CIO

Dienste müssen zentral betrieben, angeboten und bei Bedarf genutzt werden, wenn die Zentralisierung deutliche Vorteile mit sich bringt (Kosten, räumliche Sicherheit, Notstromversorgung, 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.

(M12) Betrieb dezentraler IT-Dienste mit weltweitem Zugriff

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r

Grundsätzlich sind Services, die von IT-Dienstleistungszentren der Freien Universität Berlin bereitgestellt werden, selbst betriebenen Diensten vorzuziehen. Nur wenn der benötigte Dienst nicht von Einrichtungen der Freien Universität 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 Freien Universität Berlin erreichbar sein sollen, muss über die/den zuständige/n IT-Beauftragte/n bei der zuständigen Stelle der ZEDAT beantragt werden. Der Antrag muss begründet sein.

(M13) Überprüfung der Wirksamkeit der IT-Sicherheitsmaßnahmen

Verantwortlich für Umsetzung:	Bereichsleitung, IT-Sicherheitsbeauftragter der Freien Universität Berlin

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 die Dokumentation aktualisiert werden. Bei der Vergabe von Prüfaufträgen an externe Auftragnehmer ist auf eine anerkannte Zertifizierung zu achten. Die Überprüfung ist durch den IT-Sicherheitsbeauftragten der Freien Universität zu organisieren.

(M14) 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 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 und Angaben zum Zugriff auf das Betriebshandbuch enthalten sein. Außerdem muss ein Alarmierungsplan erstellt werden, in dem die Meldewege und die Kontaktdaten der beteiligten Stellen und Personen im Notfall beschrieben sind.

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.

8.3 IT-Personal

(M15) Sorgfältige Personalauswahl

Verantwortlich für Umsetzung:	Bereichsleitung

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

(M16) Angemessene Personalausstattung

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.

Die Personalausstattung muss so bemessen sein, dass die Verfügbarkeit und Dienstqualität der IT-Infrastruktur und IT-Dienste mit zentraler Bedeutung in einem für die Freie Universität Berlin ausreichendem Maß gewährleistet ist.

(M17) 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.

Bei der Auswahl der Vertreter ist zu beachten, dass das Prinzip der Rollentrennung nicht unterlaufen wird.

(M18) Qualifizierung

Verantwortlich für Umsetzung: Bereichsleitung

IT-Personal darf 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.

8.4 Sicherung der Infrastruktur

(M19) Zugang zu Räumen mit zentraler Netzinfrastruktur

Verantwortlich für Umsetzung: Technische Abteilung

Die vollständige Zugangskontrolle zu allen Räumen, in denen Geräte mit zentraler Bedeutung für die Netzinfrastruktur der Freien Universität Berlin aufgestellt sind, liegt bei der dafür zuständigen Stelle des Hochschulrechenzentrums. Im Falle einer mehrfachen Nutzung – soweit dies mit einem sicheren Betrieb der Netzinfrastruktur vereinbar ist – entscheidet die zuständige Stelle des Hochschulrechenzentrums über die Schlüsselvergabe.

(M20) Sicherung der Serverräume

Verantwortlich für Umsetzung: Technische Abteilung

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. 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. Fremdpersonal soll sich in Serverräumen nach Möglichkeit nur unter Aufsicht aufhalten.

(M21) 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.

(M22) Sicherung der Netzknoten

Verantwortlich für Umsetzung: Hochschulrechenzentrum

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 M20.

(M23) Verkabelung und Funknetze

Verantwortlich für Umsetzung: Hochschulrechenzentrum

Die 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 der/dem zuständigen IT-Beauftragten und mit dem Hochschulrechenzentrum abzustimmen. Funknetze dürfen nur nach vorheriger Abstimmung mit dem Hochschulrechenzentrum betrieben werden.

(M24) Geschützte Kabelverlegung

Verantwortlich für Umsetzung: Technische Abteilung, Hochschulrechenzentrum

Bei der Verlegung der Leitungen muss darauf geachtet werden, dass Unbefugte keine Möglichkeit des Zugriffs haben. Offen zugänglich verlegte Leitungen sollten in Zusammenarbeit mit der für die Baumaßnahmen zuständigen Stelle in geeigneter Weise geschützt werden.

(M25) Einweisung und Beaufsichtigung von Fremdpersonal

Verantwortlich für Umsetzung: Technische Abteilung, Hochschulrechenzentrum

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.

(M26) Stromversorgung und Überspannungsschutz

Verantwortlich für Umsetzung: Technische Abteilung

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

(M27) USV

Verantwortlich für Umsetzung: Technische Abteilung, IT-Dienstleister

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.

(M28) Brandschutz

Verantwortlich für Umsetzung: Brandschutzbeauftragter, Technische Abteilung

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.

(M29) Schutz vor Wasserschäden

Verantwortlich für Umsetzung: Technische Abteilung

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.

(M30) Klimatisierung

Verantwortlich für Umsetzung: Technische Abteilung

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.

8.5 Hard- und Softwareeinsatz

(M31) Beschaffung

Verantwortlich für Umsetzung: Bereichsleitung

Der Einsatz von Soft- und Hardware ist mit der/dem zuständigen IT-Beauftragten abzustimmen. Die Beschaffung von Soft- und Hardware muss von der/vom zuständigen IT-Beauftragten genehmigt werden.

(M31a) Berücksichtigung digitaler Signaturen beim IT-Einsatz

Verantwortlich für Umsetzung: Bereichsleitung, Verfahrensverantwortliche/r

Bei der Auswahl neu zu beschaffender Software muss 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.

(M32) Softwareentwicklung

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r, IT-Projektleitung

Bei der Entwicklung von umfangreicher Software müssen die fachlichen und technischen Anforderungen vorher spezifiziert sein. Diese Arbeiten werden in enger Abstimmung mit den betroffenen Bereichen durchgeführt. Bereits in der Spezifikationsphase muss darauf geachtet werden, dass die relevanten IT-Sicherheitsaspekte berücksichtigt werden können. Bei der Verarbeitung personenbezogener Daten müssen darüber hinaus datenschutzrechtliche Anforderungen berücksichtigt werden.

Die Entwicklungsarbeiten einschließlich aller Tests müssen in separaten Testumgebungen stattfinden. Die strikte Trennung von Entwicklung und Produktion gilt insbesondere auch für die Verarbeitung von schützenswerten Daten. Vor der Überführung der Software von der Entwicklung in den Produktionsbetrieb muss die/der zuständige IT-Beauftragte informiert werden.

(M33) Separate Entwicklungsumgebung

Entfällt (integriert in M32).

(M34) Entwicklung von Software nach standardisierten Verfahren

Entfällt.

(M35) Kontrollierter Softwareeinsatz

Verantwortlich für Umsetzung: IT-Personal, Anwender

Auf Rechnersystemen der Freien Universität Berlin 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 ist nur gestattet, wenn eine Genehmigung der zuständigen Stelle vorliegt oder ein Bereich eine pauschale Freigabe für Teilbereiche festgelegt hat.

(M36) Test von Software

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r, IT-Personal

Vor dem Einsatz neuer Software oder ggf. neuer Versionen muss die Erfüllung der Anforderungen durch hinreichende Tests sichergestellt sein.

(M37) 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.

(M38) Schutz vor Schadprogrammen

Verantwortlich für Umsetzung: IT-Personal, Anwender

Auf allen Arbeitsplatz-Rechnern ist, soweit möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Regelmäßig (möglichst automatisiert) sind die Virenerkennungsmuster zu aktualisieren. Wird auf einem System schädlicher Programmcode entdeckt, muss die zuständige Stelle immer dann informiert werden, wenn die Schadsoftware nicht zuverlässig entfernt werden kann.

(M39) 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. Bei Arbeitsplatz-Rechnern ist der Zugriff auf das Rechner-BIOS durch ein Passwort zu schützen.

(M40) Dokumentation der Hard- und Software

Entfällt.

(M41) 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.

(M42) Einsatz von Diebstahl-Sicherungen

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r

Diebstahl-Sicherungen sind unter Berücksichtigung der Wirtschaftlichkeit überall dort einzusetzen, wo Werte zu schützen sind bzw. dort, wo andere Maßnahmen – beispielsweise geeignete Zutrittskontrolle zu den Arbeitsplätzen – nicht umgesetzt werden können. Diebstahl-Sicherungen sind zum Beispiel dort sinnvoll, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist.

(M43) Datenablage in der Cloud

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 entnommen werden.
Das genannte Regelwerk ist auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

8.6 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 Freien Universität Berlin in Anspruch genommen werden.[10)]

(M44) Schutz vor unbefugtem Mithören

Entfällt.

[10)] Siehe Abschnitt 1 Geltungsbereich dieser Richtlinie.

(M45) 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.

(M46) Verlust eines mobilen Dienst-Geräts

Verantwortlich für Umsetzung: Anwender

Der Verlust eines mobilen Dienst-Geräts muss sofort der Hotline gemeldet werden. 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.

(M47) Geregelte Übergabe eines mobilen Dienst-Geräts

Verantwortlich für Umsetzung: Gruppenleiter, 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.

(M48) 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.

8.7 Zugriffsschutz

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

(M49) 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.

(M50) Bereitstellung von Verschlüsselungssystemen

Verantwortlich für Umsetzung: IT-Dienstleister

Zur Absicherung besonders schützenswerter Daten, insbesondere auf mobilen Geräten, müssen geeignete Systeme (Programme oder spezielle Hardware) zur Verschlüsselung durch die IT-Dienstleister der Freien Universität Berlin bereitgestellt werden.

(M51) Netzzugänge

Verantwortlich für Umsetzung: Anwender, Bereichsleitung

Der Anschluss von Systemen über die Netzzugänge der Freien Universität Berlin hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen ist unzulässig.

(M52) Ausscheiden oder Wechsel von Mitarbeitern/innen

Verantwortlich für Umsetzung: Bereichsleitung, Vorgesetzte/r des Mitarbeiters

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass die/der zuständige IT-Beauftragte 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.

(M53) 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 darf nur in einem geregelten Verfahren erfolgen. Die Einrichtung, Freigabe und Sperrung sind zu dokumentieren.

(M54) 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 Standard-Benutzerkennungen zu verwenden.

(M55) Zentralisierung des Identity- und Passwort-Managementsystems

Verantwortlich für Umsetzung: CIO

Die IT-Dienstleister der Freien Universität Berlin sind verpflichtet, ein geeignetes System zur zentralen Identity- und Passwortverwaltung bereit zu stellen. Zur Authentifizierung und Autorisierung müssen alle zugangskontrollierten Systeme das zentral angebotene Identity- und Passwort-Managementsystem nutzen, soweit dies technisch umsetzbar und organisatorisch sinnvoll ist.

(M56) 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 IT-Personal noch externen Dienstleistern bekannt gegeben werden, zum Beispiel im Rahmen der Nutzung von E-Mail-Sammeldiensten.

(M56a) 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.
3. Das Passwort muss mindestens 5 verschiedene Zeichen und mindestens zwei Nicht-Buchstaben (Ziffern oder Sonderzeichen) enthalten.
4. Das Passwort muss mindestens 8 Zeichen lang sein.[11)]
5. Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr verwendet werden.

[11)] Durch die Wahl eines längeren Passworts kann die Sicherheit des Passworts deutlich erhöht werden.

(M56b) 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 Freien Universität Berlin 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 werden, muss 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).

(M56c) Administration von Passwörtern

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r

1. Falls technisch möglich, sollten die Bildungsregeln aus (M56a) erzwungen werden.
2. Jede/r Benutzer/in muss ihr/sein eigenes Passwort jederzeit ändern können.
3. Das Passwort darf nicht länger als die Anzahl der signifikanten Stellen sein.
4. 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.
5. Bei der Authentifizierung in vernetzten Systemen dürfen Passwörter nicht unverschlüsselt übertragen werden.
6. Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

(M56d) 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.

(M56e) 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.

(M57) 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.

(M58) Änderung der Zugriffsrechte

Entfällt (integriert in M32).

(M59) Abmelden und ausschalten

Verantwortlich für Umsetzung: Anwender, IT-Personal

Bei Verlassen des Raumes muss der Zugriff auf das IT-System durch einen Kennwortschutz gesperrt werden. 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.

(M60) Verwendung dienstlicher E-Mail-Adressen

Verantwortlich für Umsetzung: Anwender, IT-Personal

Für dienstliche Belange muss die dienstliche E-Mail-Adresse der Freien Universität Berlin 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 Freien Universität Berlin betrieben werden, ist nicht zulässig.

(M60a) Fernwartung

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

Bei einer Vereinbarung zur Fernwartung muss neben den datenschutzrechtlichen Erfordernissen auch der Handlungsleitfaden „Zugriff auf schützenswerte Daten der Freien Universität Berlin durch Externe“ beachtet werden. Der Handlungsleitfaden ist

auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

8.8 Protokollierung

Eine angemessene Protokollierung von IT-Aktivitäten und -Ereignissen ist ein wesentlicher Faktor der Betriebssicherheit. 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.

(M61) 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 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 dem Berliner Datenschutzgesetz muss beachtet werden.

(M61a) 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 (M61).

(M62) 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 dem Berliner Datenschutzgesetz zu beachten.

8.9 System- und Netzwerkmanagement

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

(M63) Sichere Netzwerkadministration

Verantwortlich für Umsetzung: IT-Personal, Hochschulrechenzentrum

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.

(M64) Netzmonitoring

Verantwortlich für Umsetzung: IT-Personal, Hochschulrechenzentrum

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.

(M65) Verhinderung des unbefugten Netzzugangs

Verantwortlich für Umsetzung: IT-Personal, Hochschulrechenzentrum

Netzwerkzugänge sind so zu konfigurieren, dass ein unbefugter Zugang zum Netz der Freien Universität Berlin verhindert wird.

(M66) Kommunikation zwischen unterschiedlichen Sicherheitsniveaus

Verantwortlich für Umsetzung: IT-Personal, Hochschulrechenzentrum

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 Freien Universität Berlin sind nicht gestattet. Falls auf Grund besonderer Umstände die Installation anderer Kommunikationswege unumgänglich ist, muss dies zuvor durch die zuständige Stelle genehmigt werden. Jeder Zugriff Externer ist zu protokollieren.

(M67) Rechnernamen

Verantwortlich für Umsetzung: IT-Personal, IT-Dienstleister

Zur Erleichterung der Notfallvorsorge und der Missbrauchsnachverfolgung muss jedes Gerät, das mit den Netzen der Freien Universität Berlin verbunden ist, einen DNS-Eintrag (DNS = Domain Name System) der Freien Universität Berlin besitzen.

8.10 Datensicherung

(M68) Datensicherungskonzept

Verantwortlich für Umsetzung: Verfahrensverantwortliche/r

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 erfolgt. 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 sind zu dokumentieren (Datum, Art der Durchführung der Sicherung/gewählte Parameter, Beschriftung der Datenträger, Ort der Aufbewahrung).

(M69) 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.

(M70) 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.

(M71) Verifizierung der Datensicherung

Verantwortlich für Umsetzung: IT-Personal

Die Konsistenz der Datensicherungsläufe ist sicher zu stellen, d. h. die Lesbarkeit der Datensicherung ist zu überprüfen. Das testweise Wiedereinspielen von Datensicherungen soll wenigstens einmal jährlich erfolgen.

8.11 Datenträgerkontrolle

(M72) 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 eingeplant werden, das für die verwendeten Datenformate geeignet ist.

(M73) 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.

(M74) 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 Freien Universität 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.

(M75) 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.

(M76) 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. (Siehe dazu Handlungsleitfaden „Zugriff auf schützenswerte Daten der Freien Universität Berlin durch Externe“)
Das genannte Regelwerk ist auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

(M77) Sichere Entsorgung vertraulicher Papiere

Verantwortlich für Umsetzung: Anwender

Papiere mit vertraulichem Inhalt sind mit Hilfe eines Aktenvernichters zu vernichten. Bei der Beschaffung eines Aktenvernichters sind die geltenden Normvorschriften zu beachten. Alternativ kann die Entsorgung auch über einen Dienstleister erfolgen. In diesem Fall muss sichergestellt sein, dass der Auftragnehmer über entsprechende Zertifikate verfügt. Der Auftragnehmer ist zur Protokollierung der Aktenvernichtung zu verpflichten.

8.12 Verschiedenes

(M78) Einsatz von Videokonferenztechnik bei Prüfungen

Verantwortlich für Umsetzung: Anwender

Der Einsatz von Videotechnik bei mündlichen Prüfungen und Disputationen ist nur in begründeten Ausnahmefällen erlaubt. Bei der Entscheidung über die Zulässigkeit von Videokonferenztechnik sind die Hinweise des Rechtsamts der Freien Universität Berlin zu beachten.
Die genannten Hinweise sind auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

(M79) Einsatz von Videokonferenztechnik bei Bewerbungsgesprächen

Verantwortlich für Umsetzung: Anwender

Beim Einsatz von Videokonferenztechnik bei Bewerbungsgesprächen müssen datenschutzrechtliche Anforderungen beachtet werden, insbesondere muss die freiwillige Einwilligung des Betroffenen vorliegen. Die Durchführung eines Video-Bewerbungsgesprächs stellt eine Verarbeitung von personenbezogenen Daten dar und muss inkl. der

Einwilligung des Betroffenen gemäß den Anforderungen der Datenschutz-Grundverordnung dokumentiert werden. Bei der Auswahl der eingesetzten Technik ist auf die Gewährleistung der Vertraulichkeit zu achten. Es sollte Technik eingesetzt werden, die die Kommunikation durch eine sogenannte Ende-zu-Ende-Verschlüsselung schützt.

(M80) Einsatz von Social Media Diensten

Verantwortlich für Umsetzung: Anwender

Für den Einsatz von Social Media zur Kommunikation und Publikation existieren verschiedene Regelwerke, die zu beachten sind:

- Grundregeln zur offiziellen Verwendung von sozialen Netzwerken durch Einrichtungen und Mitarbeiter/innen der Freien Universität Berlin
- Grundregeln zum Einsatz von iTunes U an der Freien Universität Berlin
- Grundregeln zum Einsatz von Online-Diensten der Freien Universität Berlin zur Information, Kommunikation oder Publikation im Internet (Internet-Online-Dienste)

Alle genannten Regelwerke sind auf den Webseiten zur IT-Sicherheit unter „DOWNLOADS“ (siehe Abschnitt 14) abrufbar.

Teil IV Ausführungsbestimmungen

Aufgrund der hohen Eigenständigkeit der einzelnen Bereiche wird – in Übereinstimmung mit Abschnitt 3 – die Verantwortung für die Umsetzung der IT-Sicherheitsrichtlinie auf die einzelnen Bereiche der Freien Universität übertragen. Wesentliche Impulse zur Unterstützung der Verantwortlichen gehen dabei von den IT-Beauftragten aus.

9 Inkraftsetzung und Aktualisierung der IT-Sicherheitsrichtlinie

Das Präsidium der Freien Universität Berlin setzt die IT-Sicherheitsrichtlinie in Kraft.

Die IT-Sicherheitsrichtlinie bedarf der regelmäßigen Überprüfung und Überarbeitung. Das Präsidium der Freien Universität Berlin hat die Arbeitsgruppe IT-Sicherheit mit der Pflege und Fortschreibung der IT-Sicherheitsrichtlinie beauftragt. Die Gewährleistung der Aktualität wird durch die folgende Vorgehensweise sichergestellt:

1.	Entwurf einer neuen Richtlinie	Die Arbeitsgruppe überarbeitet die Richtlinie und erstellt einen Entwurf einer neuen IT-Sicherheitsrichtlinie.
2.	Abstimmung	Die Arbeitsgruppe stimmt den Entwurf mit CIO, Personalvertretung, Datenschutzbeauftragten und IT-Beauftragten ab.
3.	Vorlage im Präsidium	Die Arbeitsgruppe legt dem Präsidium den abgestimmten Richtlinienentwurf vor.
4.	Prüfung und In-Kraft-Setzung	Das Präsidium prüft den Entwurf und setzt ihn in Kraft.

10 Konfliktlösung bei der Umsetzung der IT-Sicherheitsrichtlinie

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

Stellt eine Stelle in der Freien Universität Berlin einen Sicherheitsmangel in einem IT-Verfahren fest, der zu gravierenden Schäden führen kann, ist der IT-Sicherheitsbeauftragte der Freien Universität 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 den CIO. Der CIO entscheidet über das weitere Vorgehen.

Anhang

11 Glossar

Zur Gewährleistung einheitlicher Begriffsdefinitionen in allen IT-Regelwerken ist das Glossar als separates Dokument vorhanden, so dass unterschiedliche Regelwerke darauf verweisen können:

https://www.fu-berlin.de/sites/it-sicherheit/downloads/Glossar/index.html (HTML)
https://www.fu-berlin.de/sites/it-sicherheit/downloads/Global-Glossar.pdf (PDF)

12 Abbildungsverzeichnis

13 Tabellenverzeichnis

14 Literaturverzeichnis

Damit die Verweise auf andere Dokumente so aktuell wie möglich angegeben werden können, wird an dieser Stelle lediglich auf die Webseite zur IT-Sicherheit an der Freien Universität Berlin verwiesen:

https://www.fu-berlin.de/sites/it-sicherheit/

Alle IT-Regelwerke und Dienstvereinbarungen mit IT-Bezug werden auf dieser Webseite unter der Rubrik „DOWNLOADS“ aufgelistet.