Freie Universität Berlin

IT-Sicherheitsrichtlinie
für die
Freie Universität Berlin

Version 2.0

25. Februar 2008

Gliederung

Inhaltsverzeichnis

Vorbemerkung

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

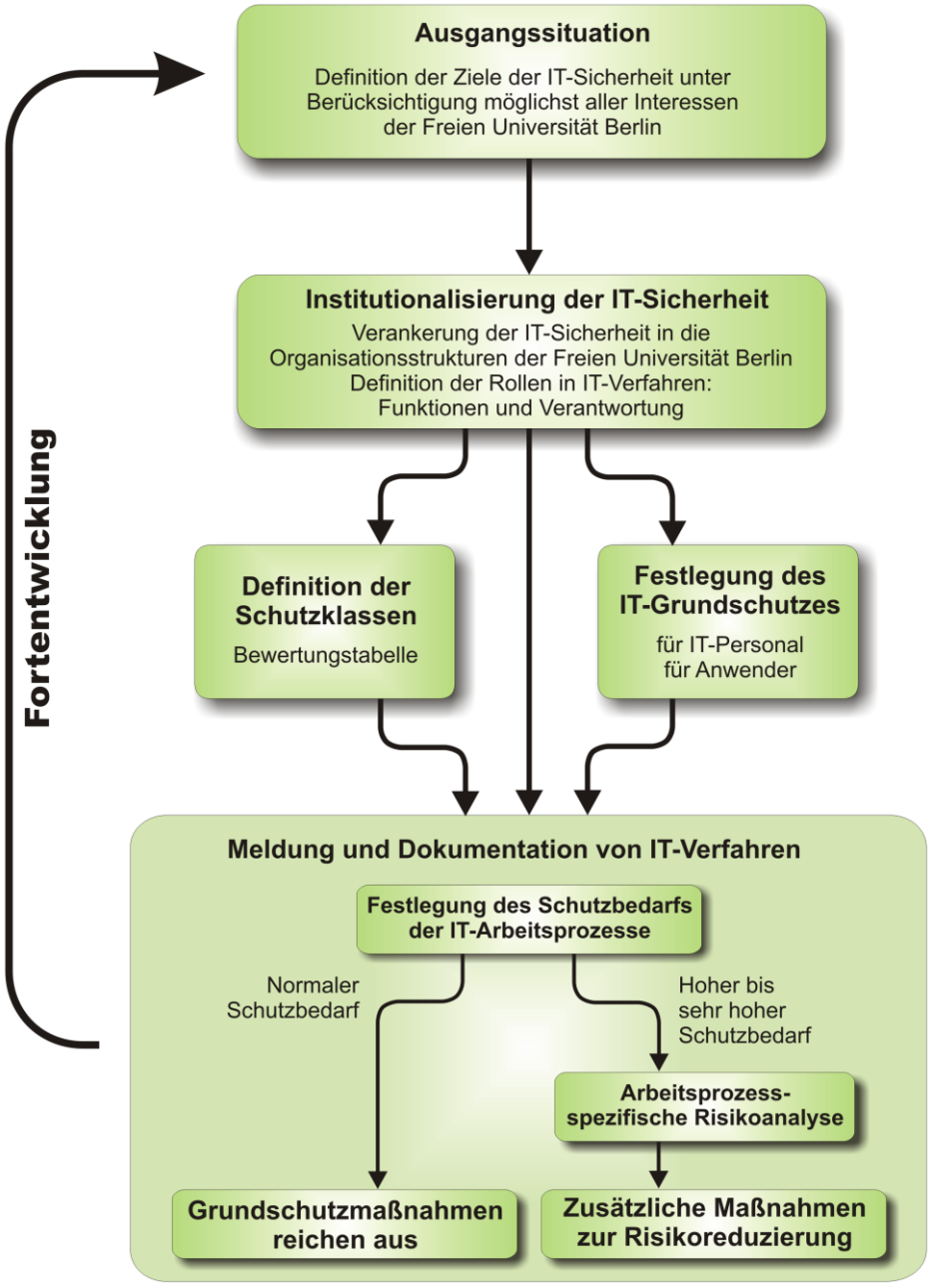


Abbildung 1: Modell des IT-Sicherheitsprozesses

Die Gliederung der vorliegenden Richtlinie orientiert sich an der Abfolge der Schritte im IT-Sicherheitsprozess. Zur besseren Orientierung wird das Bild des IT-Sicherheitsprozesses zu Beginn der einzelnen Hauptabschnitte wiederholt. Die jeweils behandelten Abschnitte werden im Bild besonders hervorgehoben.

Die in dieser IT-Sicherheitsrichtlinie beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind für die Einrichtungen der Freien Universität Berlin verbindlich.

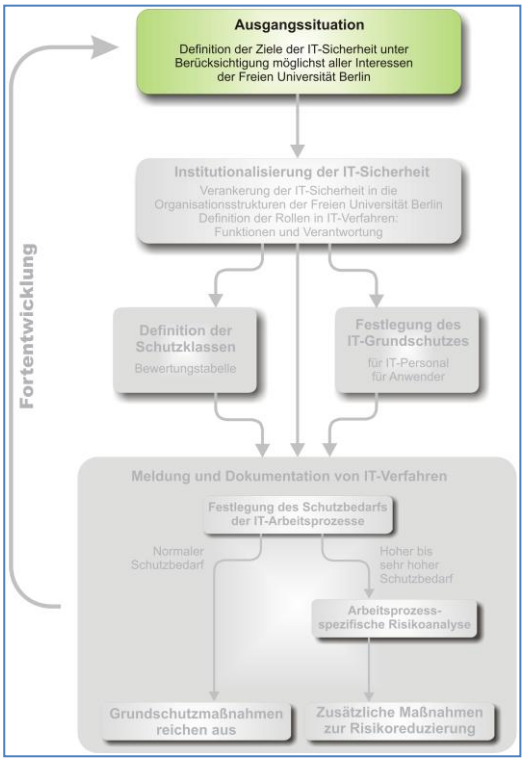
In diesem Dokument wird die Formulierung „Organisationseinheit“ als Sammelbegriff verwendet und umfasst alle Einrichtungen der Freien Universität Berlin, einschließlich der Fachbereiche, Zentralinstitute und Zentraleinrichtungen sowie den Bereichen und Abteilungen der Zentralen Universitätsverwaltung und des Präsidiums.

Des Weiteren wird aus Gründen der Einfachheit und des Textflusses durchgehend die männliche Anredeform verwendet. Sie soll kein bestimmtes Geschlecht bevorzugen oder benachteiligen.

1. Ausgangssituation

Die Freie Universität Berlin setzt in hohem Maße IT-Verfahren in ihren Kernprozessen ein:

- Forschung: zum Beispiel weltweite Kommunikation und Zusammenarbeit, elektronische Publikation und Recherche, rechenintensive Anwendungen, IT-gestützte Messverfahren mit hohem Datenaufkommen
- Lehre: zum Beispiel e-Learning, das Bibliothekssystem ALEPH500 mit seinen Subsystemen (Dokumentenserver, Angebot digitaler Bibliotheken etc.)



- Verwaltung: zum Beispiel Verwaltung von Personal-, Studierenden- und Prüfungsdaten, Finanzsteuerung

Verbunden mit dem steigenden 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

- gesetzlichen Anforderungen: zum Beispiel Datenschutz, Haushaltsrecht und Steuerrecht
- vertraglichen Anforderungen: zum Beispiel die Nutzung des DFN-Netzes und die Revisionspflicht gegenüber Drittmittelgebern
- Selbstverpflichtung: zum Beispiel Ehrenkodex 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 und die Verfügbarkeit, Vertraulichkeit und Integrität der Daten sicherstellen. Die Maßnahmen sollen Schadensereignisse abwehren und so Schäden vermeiden, die durch höhere Gewalt, technisches Versagen, Nachlässigkeit oder Fahrlässigkeit drohen.

Die Mitarbeiter der Freien Universität werden grundsätzlich als vertrauenswürdig angesehen. Eine Überwachung oder auch nur Verfolgung aller Aktivitäten im Netz ist weder notwendig noch wünschenswert. Ein vertrauensvolles und konstruktives Arbeitsklima, in dem Teamgeist und Eigenverantwortung einen hohen Stellenwert be-

sitzen, bildet die beste Grundlage für einen weitestgehend reibungslosen, sicheren und effektiven Gebrauch der Informationstechnik.

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

Die 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 können drohende Gefahren erfolgreich abgewehrt werden. Welche Schutzmaßnahmen zu treffen sind, ist in der vorliegenden IT-Sicherheitsrichtlinie verbindlich beschrieben.

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

Die Beschreibung aller IT-Verfahren (siehe Abschnitt 1.2) ist ein wesentlicher Bestandteil des IT-Sicherheitsprozesses an der Freien Universität Berlin. Den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) folgend, wird unterschieden zwischen Verfahren, deren Schutzbedarf bezüglich Vertraulichkeit, Integrität und Verfügbarkeit im Rahmen des Normalmaßes liegen, sowie Verfahren mit höherem Schutzbedarf. Für die Festlegung des Schutzbedarfs ist eine Schutzbedarfsanalyse (siehe Kapitel 3) durchzuführen.

Die zur Erreichung des Grundschutzes erforderlichen Maßnahmen werden unabhängig von den einzelnen Verfahren beschrieben. Der Grundschutz ist unterteilt in einen Bereich für IT-Anwender und für IT-Personal. Als IT-Anwender werden im Folgenden alle Beschäftigten der Freien Universität Berlin, einschließlich der studentischen Hilfskräfte, verstanden. Der Begriff IT-Personal bezeichnet alle Beschäftigten der Freien Universität Berlin, deren Tätigkeitsfelder ganz oder teilweise im Bereich der IT angesiedelt sind (zum Beispiel Administratoren und Applikationsbetreuer). Die Studierenden der Freien Universität Berlin unterliegen den jeweils geltenden Benutzerordnungen. Der für jeden IT-Arbeitsplatz zu erreichende Grundschutz bildet das Fundament der IT-Sicherheit der Freien Universität Berlin. Für IT-Verfahren mit höherem Schutzbedarf müssen über diese Grundschutz-Sicherheitsmaßnahmen hinaus zusätzliche verfahrens- bzw. arbeitsprozessbezogene Maßnahmen erarbeitet werden, die aus entsprechenden Risikoanalysen abgeleitet werden.

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

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

1.1. Grundbegriffe der IT-Sicherheitsrichtlinie

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

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

- **IT-Verfahren**
  Ein IT-Verfahren ist eine Zusammenfassung von einem oder mehreren Arbeitsprozessen, die sich auf IT stützen. Die zusammengefassten Arbeitsprozesse bilden eine arbeitsorganisatorisch abgeschlossene Einheit und verfolgen ein gemeinsames Ziel.

- **Verfügbarkeit**
  Verfügbarkeit bezieht sich auf Daten und Verfahren und bedeutet, dass sie zeitgerecht zur Verfügung stehen.

- **Vertraulichkeit**
  Vertraulichkeit ist gewährleistet, wenn nur diejenigen von Daten Kenntnis nehmen können, die dazu berechtigt sind. Daten dürfen weder unbefugt gewonnen noch ungewollt offenbart werden.

- **Integrität**
  Integrität ist gewährleistet, wenn Daten unversehrt und vollständig bleiben.

- **Authentizität**
  Authentizität bedeutet, dass Daten jederzeit ihrem Ursprung zugeordnet werden können.

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

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

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

1.2. IT-Verfahren und Arbeitsprozesse

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

Abbildung 2: Beispiel für die Erfassung von IT-gestützten Arbeitsprozessen durch IT-Verfahren. Ein gelbes Sechseck symbolisiert ein IT-Verfahren. Ein graues Sechseck soll einen bzw. mehrere Arbeitsprozesse symbolisieren. Mit der Erfassung und Dokumentation aller IT-Verfahren wird der IT-Einsatz in der Freien Universität Berlin vollständig abgebildet.

1.2.1. Erfassung und Dokumentation von IT-Verfahren

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

I. Zweck des IT-Verfahrens, Beschreibung der Arbeitsabläufe und Angaben über die gesetzliche Grundlage

II. Schutzbedarfsanalyse

III. Risikoanalyse in Abhängigkeit vom Ergebnis der Schutzbedarfsanalyse

IV. Beschreibung der Rollen

V. Angaben über die Anzahl und Art von technischen Einrichtungen und Geräten (Mengengerüst)

VI. Angaben der Schnittstellen zu anderen IT-Verfahren, IT-Systemen und sonstigen Diensten

VII. Angaben über die vom IT-Verfahren betroffenen Organisationseinheiten

VIII. Aufstellungsort von Anlagen und Geräten, die wesentliche Funktionen innerhalb des Arbeitsprozesses bzw. IT-Verfahrens erfüllen; alle weiteren Anlagen und Geräte müssen lediglich zahlenmäßig erfasst und einer Unterorganisationseinheit zugewiesen werden

IX. Betriebskonzept mit allen für den Betrieb notwendigen Angaben über die im IT-Verfahren erfassten technischen Systeme

X. Soweit personenbezogene Daten der Beschäftigten automatisiert verarbeitet werden: Angaben über den Umgang mit personenbezogenen Daten (Datenschutzmeldung gemäß § 19 II BlnDSG bzw. § 2 Abs. 3 Informationsverarbeitungsgesetz (IVG))

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

Abweichend von den vorangegangenen Dokumentationskriterien gilt für den Betrieb von IT-Systemen in Forschungsprojekten und für IT-Systeme mit kurzer Betriebsdauer (weniger als sechs Monate) keine Pflicht zur ausführlichen Verfahrensbeschreibung. Hauptsächlich muss lediglich der Betrieb angezeigt werden. Die in diesem Fall geltenden Regeln sind in der IT-Rahmendienstvereinbarung im § 10 „IT-Systeme in Forschungsprojekten sowie IT-Systeme mit kurzer Lebensdauer“ beschrieben.

Auch wenn für IT-Systeme in Forschungsprojekten und für IT-Systeme mit kurzer Betriebsdauer keine Verpflichtung zur Durchführung einer Schutzbedarfsanalyse und ggf. einer Risikoanalyse bestehen, muss dennoch die Sicherheit aller betroffenen Systeme sowie der zugrunde liegenden Infrastruktur gewährleistet werden. Beispielsweise können speziell dafür ausgelegte Netzwerke, die gegenüber anderen Netzwerken abgeschottet sind, bereit gestellt werden. Auch der Einsatz virtueller Serversysteme kann neben anderen Maßnahmen zur Erhöhung der Sicherheit beitragen.

Weitere Merkmale eines IT-Verfahrens sind der längerfristige Charakter der erfassten IT-gestützten Arbeitsabläufe. Ein IT-Verfahren wird üblicherweise über mehrere Jahre hinweg betrieben. Bei der Festlegung von IT-Arbeitsprozessen wie auch von

IT-Verfahren soll der Grundsatz der Generalisierung bzw. der Zusammenfassung beachtet werden. Der IT-Arbeitsprozess bildet bei der Erfassung des IT-Einsatzes die kleinste Einheit und ist als eine sequenzielle und/oder parallele Abfolge von zusammenhängenden IT-gestützten und/oder IT-unterstützenden Tätigkeiten definiert. Als Anhaltspunkt für eine Zusammenfassung oder eine Trennung von Arbeitsabläufen können u. a. folgende Kriterien dienen:

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

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

- Beispiel für ein IT-Verfahren mit nur einem Arbeitsprozess: PC-Pool
  Der Betrieb eines PC-Pools beinhaltet typischerweise nur einige wenige Tätigkeiten, die alle der Bereitstellung von PCs dienen. Die Aufteilung der Tätigkeiten in verschiedene Arbeitsprozesse ist nicht sinnvoll, da beispielsweise auf die einzelnen Arbeitsprozesse das Rollenmodell nicht mehr sinnvoll angewendet werden kann.

- Beispiel für ein IT-Verfahren mit mehreren Arbeitsprozessen: Campus Management
  Das Campus-Management-System umfasst eine Vielzahl von zusammenhängenden Prozessen in verschiedenen Organisationseinheiten der Freien Universität Berlin. Beispielsweise müssen zu Beginn eines Semesters die Anmeldevorgänge der Studierenden zu den Lehrveranstaltungen und am Ende eines Semesters die Prüfungsergebnisse erstellt und verwaltet werden. Beide Prozesse sind relativ komplex und beinhalten eine Reihe von verschiedenen Abläufen in unterschiedlichen Einrichtungen (Immatrikulationsamt, Prüfungsbüros in den Fachbereichen usw.) mit verschiedenen Akteuren (Mitarbeiter im Immatrikulationsamt und in den Prüfungsbüros, Dozenten usw.). In beiden Prozessen werden auch unterschiedliche Daten verarbeitet. Zu einem sind es Stammdaten der Studierenden, Angaben zu Lehrveranstaltungen usw. Im zweiten Fall werden vor allem Prüfungsdaten verarbeitet. Aus diesen Gründen wäre in diesem Beispiel die Aufteilung in zwei Arbeitsprozesse empfehlenswert.

Allgemein gilt, dass es normalerweise nicht sinnvoll ist, einzelne Tätigkeiten, wie z.B. die Erledigung der Korrespondenz, als einen eigenen Arbeitsprozess oder sogar als ein eigenes IT-Verfahren festzulegen. Dadurch würde eine große Zahl von IT-

Arbeitsprozessen bzw. -Verfahren entstehen, deren strukturierte Bearbeitung kaum mehr leistbar ist.

Im jährlichen Turnus, jeweils zum 1. März, sind alle Bereiche, die IT-Verfahren gemeldet haben, zur Aktualisierung der gemeldeten Daten verpflichtet. Dazu muss eine Änderungsmeldung an die durch die Leitung der Freien Universität Berlin beauftragten Stelle, zur Zeit eAS, erfolgen. Die Änderungsmeldung muss erfolgen durch die

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

1.2.2. Rollen

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

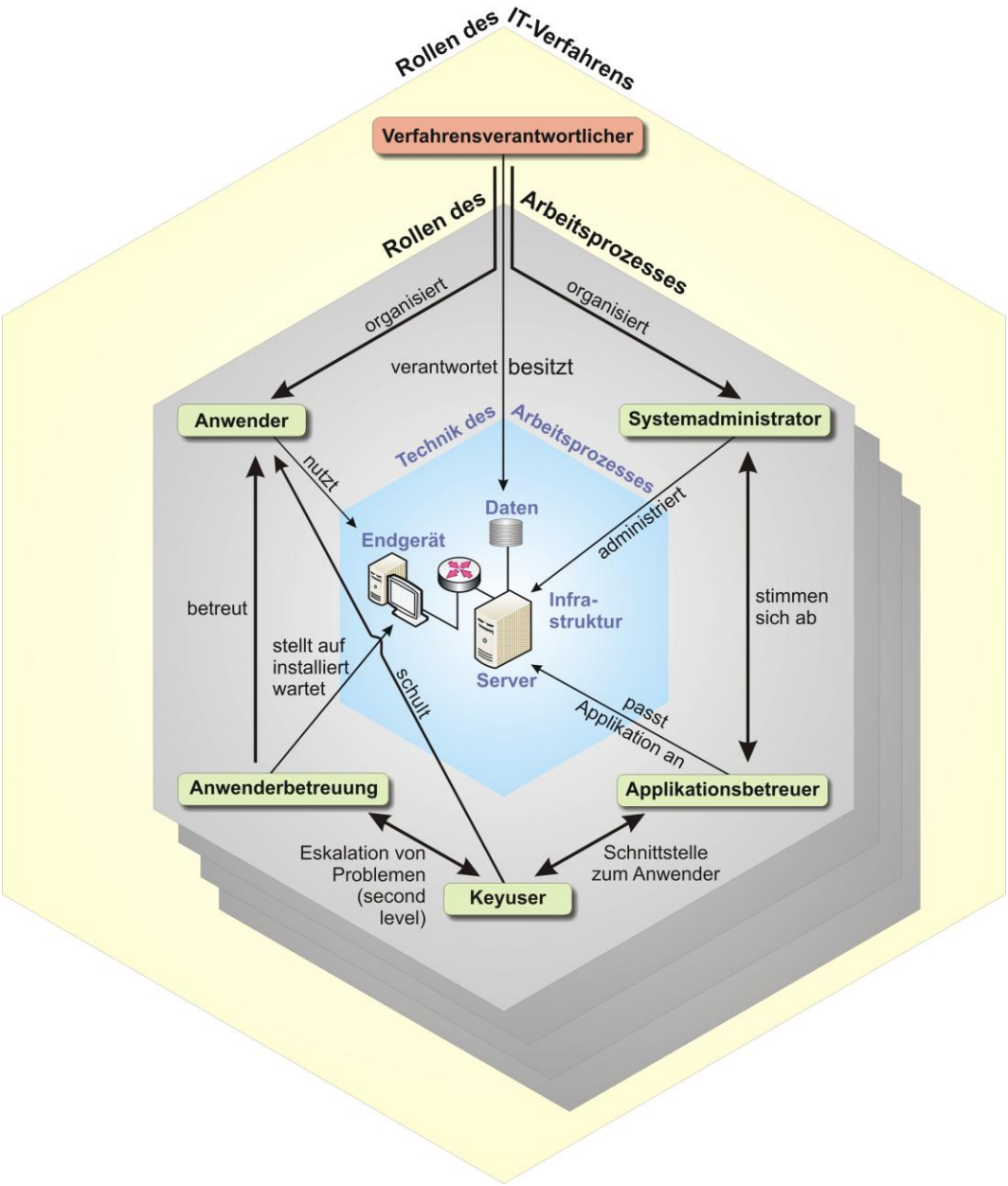


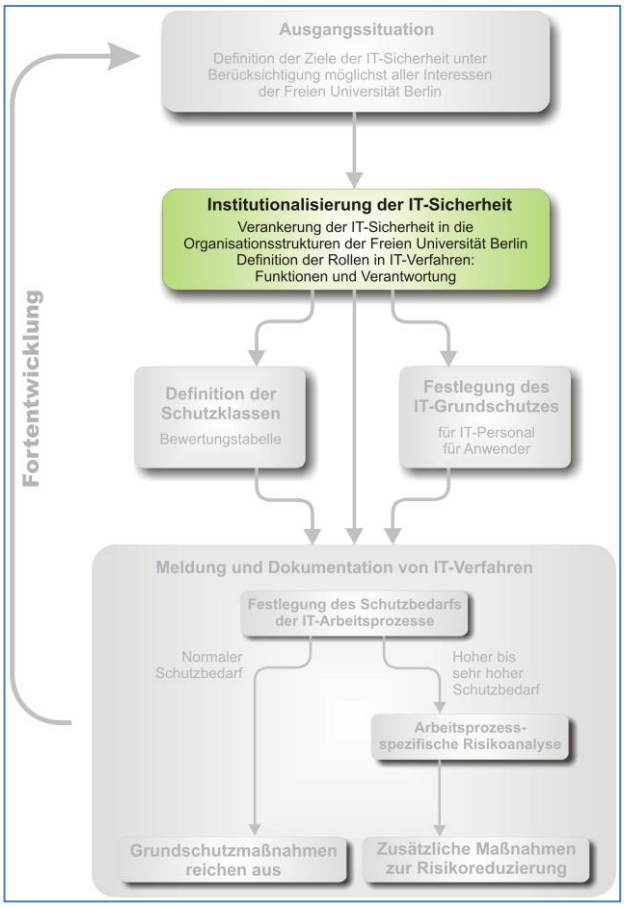
Abbildung 3: Darstellung der wichtigsten Rollen (keine Personen) innerhalb eines IT-Arbeitsprozesses und eines IT-Verfahren. Die dunkelgrau hintereinander geschachtelten Waben sollen andeuten, dass zu einem IT-Verfahren (gelbe Wabe) mehrere IT-Arbeitsprozesse gehören können.

Eine Rolle kann als Bündelung von Kompetenzen aufgefasst werden, die zur Bearbeitung von Aufgaben innerhalb eines IT-gestützten Geschäftsprozesses benötigt werden. Eine Rolle beschreibt somit, für welche Aufgaben man mit welchen Rechten auf welche Ressourcen zugreift.

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

Die an der Freien Universität Berlin verbindliche Beschreibung aller Rollen im IT-Bereich beinhaltet die IT-Organisationsrichtlinie der Freien Universität Berlin.

1.3. Verantwortlichkeiten und Organisation der IT-Sicherheit



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

Die 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 sollen an dieser Stelle kurz dargestellt werden:

- **Präsidium / Präsident**
  Das Präsidium bzw. der Präsident sind die höchste Entscheidungsinstanz an der Freien Universität Berlin in allen IT-Fragen.
- **CIO (Chief Information Officer)-Gremium**
  Neben der Durchführung übergeordneter IT-Controllingaufgaben bildet das CIO-Gremium die höchste Entscheidungsinstanz für alle IT-Vorhaben der Freien Universität Berlin mit bereichsübergreifendem Charakter und nimmt im Auftrag des Präsidiums die Verantwortung für strategische IT-Fragen an der Freien Universität Berlin wahr.
- **Zentrale IT-Dienstleister**
  Zentrale IT-Dienstleister planen, realisieren, betreiben, gestalten und stellen IT-Infrastrukturen und IT-Services für die Einrichtungen der Freien Universität bereit. IT-Dienstleister im Sinne dieser Begriffsbestimmung sind die Zentraleinrichtung für Datenverarbeitung (ZEDAT), die Universitätsbibliothek (UB),

das Center für Digitale Systeme (CeDiS) sowie die Organisationseinheit elektronische Administration und Services (eAS).

- **IT-Sicherheitsbeauftragter**
  Die Rolle des IT-Sicherheitsbeauftragten wird dem Kanzler der Freien Universität Berlin übertragen. Der Kanzler beauftragt einen Mitarbeiter mit der Wahrnehmung der Aufgaben des IT-Sicherheitsbeauftragten.

  Zu den Aufgaben des IT-Sicherheitsbeauftragten gehören:

  - Den Sicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
  - die Leitungsebene bei der Erstellung der IT-Sicherheitsrichtlinie zu unterstützen,
  - die Erstellung der IT-Sicherheitsrichtlinie, des Notfallkonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren.

- **Bereichsleitung**
  Die Leitung einer Organisationseinheit trägt die Verantwortung für den laufenden IT-Einsatz in ihrem Aufgabenbereich sowie für alle bereichsinternen IT-Planungen. Die Bereichsleitung gibt auf Grund der Ergebnisse der Schutzbedarfs- und ggf. Risikoanalyse den Betrieb des IT-Verfahrens frei. Sie benennt in Abstimmung mit dem CIO-Gremium einen IT-Verantwortlichen, der in ihrem Auftrag den IT-Einsatz koordiniert und plant und darüber hinaus die in der IT-Sicherheitsrichtlinie formulierten Maßnahmen umsetzt.

- **IT-Verantwortliche**
  Zu den zentralen Aufgaben eines IT-Verantwortlichen gehören:

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

- **AG IT-Sicherheit**
  Die Arbeitsgruppe IT-Sicherheit setzt sich aus Vertretern verschiedener Organisationseinheiten der Freien Universität zusammen. Die Zusammensetzung soll möglichst die Vielfalt der unterschiedlichen Anforderungen der Organisationseinheiten (Forschung und Lehre, Dienstleister, Verwaltung) an den IT-Einsatz berücksichtigen.

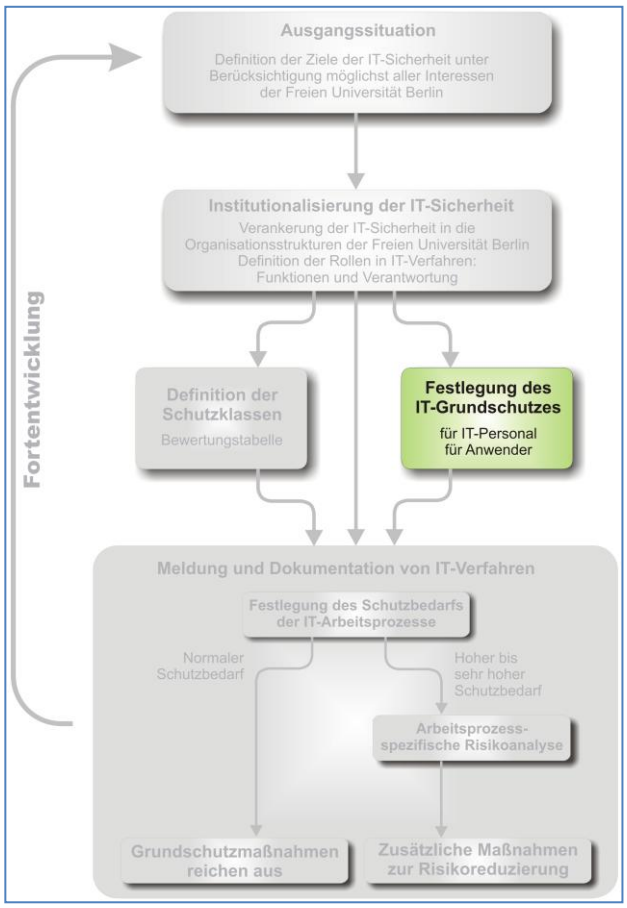
  Der IT-Sicherheitsbeauftragte schlägt dem CIO-Gremium einen Mitarbeiter als neues Mitglied in der Arbeitsgruppe IT-Sicherheit vor. Das CIO-Gremium prüft diesen Vorschlag. Nach einer Zustimmung wird der betreffende Mitarbeiter in die Arbeitsgruppe IT-Sicherheit aufgenommen.

  Zu den zentralen Aufgaben der AG IT-Sicherheit gehören:

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

  Hierbei berücksichtigt sie Datenschutz- und Mitbestimmungsaspekte.

2. Definition des Grundschutzes



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

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

Die hier für den Grundschutz zusammengestellten Maßnahmen gewährleisten ausreichende Sicherheit bei normalem Schutzbedarf. Sie bilden die Grundlage für alle IT-Verfahren / IT-Arbeitsprozesse der Freien Universität Berlin. Ihre Realisierung in den Organisationseinheiten ist notwendige, aber nicht immer hinreichende Voraussetzung für die Teilnahme an übergreifenden IT-Verfahren wie der Nutzung zentraler Dienste, zum Beispiel E-Mail, Internet oder dem Identitätsmanagement der Freien Universität Berlin (FUDIS).

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

Für IT-Verfahren mit einem Schutzbedarf „normal“ ist die Umsetzung der Grundschutzmaßnahmen zum Erreichen eines angemessenen Sicherheitsniveaus ausreichend. Für IT-Verfahren mit hohem und sehr hohem Schutzbedarf müssen über diese Grundschutzmaßnahmen hinaus zusätzliche, aus entsprechenden Risikoanalysen abgeleitete und verfahrensbezogene Maßnahmen erarbeitet werden (Zur Erarbeitung von IT-Sicherheitskonzepten für einzelne Verfahren siehe Teil 5 „Umsetzung der IT-Sicherheitsrichtlinie“). In einigen wenigen Maßnahmen werden über die Erfordernisse des Grundschutzes hinausreichende Handlungsempfehlungen gegeben. Dies betrifft die Maßnahmen M1.17, M1.18, M2.16, M2.33, M2.37, M2.48 und M2.58. Diese Maßnahmen beinhalten Hinweise zum Umgang mit besonders schützenswerten Daten.

Die Maßnahmen des Grundschutzes werden gesondert für IT-Anwender und für IT-Personal dargestellt. Der Maßnahmenkatalog ist allen Anwendern an der Freien Universität Berlin in geeigneter Weise bekannt zu geben. Die Maßnahmen des Grundschutzes für IT-Personal wenden sich unter anderem an IT-Betreuer und Systemadministratoren, die darin Vorgaben für ihre Arbeit finden.

Als Basis für die hier dargestellten IT-Grundschutzmaßnahmen dienen die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die dort beschriebenen Maßnahmen wurden den Besonderheiten der Freien Universität Berlin angepasst. Bei Fragen zu einzelnen Maßnahmen werden die detaillierten Ausführungen in den IT-Grundschutzkatalogen bzw. die Erläuterungen in der Broschüre „Informationen zum IT-Grundschutz“ empfohlen. Insbesondere beinhalten die BSI-Grundschutzkataloge detaillierte Ausführungen zur Konfiguration von unterschiedlichen Servertypen. Daher wurde auf die detaillierte Behandlung der verschiedenen Servertypen verzichtet.

Zum Zweck der Zuordnung von Verantwortlichkeiten sind zu jeder Regel und zu jeder Maßnahme die Verantwortlichen für die Initiierung und die Verantwortlichen für die Umsetzung benannt. Bei der Initiierung muss unterschieden werden zwischen dem bereichsweise zuständigen IT-Verantwortlichen und dem Verfahrensverantwortlichen.

„Verantwortlich für die Initiierung“ bezeichnet die Personen (Rolleninhaber), die die Implementierung einer Maßnahme veranlassen sollen. „Verantwortlich für die Umsetzung“ bezeichnet die Personen (Rolleninhaber), die die Realisierung der Maßnahme in der täglichen Praxis durchführen sollen.

Auf die Behandlung einiger Sicherheitsmaßnahmen zu speziellen Themen wird bewusst verzichtet. Maßnahmen, die sich mit der Absicherung von Rechenzentren beschäftigen werden nicht aufgeführt, weil es an der Freien Universität Berlin nur wenige derartige Einrichtungen gibt und dementsprechend nur wenige Mitarbeiter von dieser Thematik betroffen sind. Aus dem gleichen Grund wird auch nicht näher auf Aspekte der Netzinfrastruktur eingegangen. Die Pflege und Wartung aller bereichsübergreifenden Netze ist in der ZEDAT bei der dort zuständigen Arbeitsgruppe konzentriert, so dass auch hier wieder nur wenige Mitarbeiter betroffen sind. Die beson-

dere Problematik in Zusammenhang mit der Einrichtung und Nutzung häuslicher IT-Arbeitsplätze wird zur Zeit an der Freien Universität Berlin diskutiert. Unter welchen Bedingungen und in welchem Umfang häusliche IT-Arbeitsplätze genutzt werden dürfen, ist noch nicht abschließend geklärt. Ohne Kenntnis der Rahmenbedingungen ist es deshalb nicht sinnvoll, Maßnahmen zur Sicherheit zu formulieren.

2.1. Maßnahmen des IT-Grundschutzes für IT-Anwender

2.1.1. Allgemeines

- **Anwenderqualifizierung (M1.1)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)

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

- **Meldung von Sicherheitsproblemen (M1.2)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Verantwortlicher (bereichsspezifisch), Verfahrensverantwortlicher (verfahrensspezifisch)

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

2.1.2. Sicherung der Infrastruktur

- **Räumlicher Zugangsschutz (M1.3)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

- **Brandschutz (M1.4)**

Verantwortlich für Initiierung:	Brandschutzbeauftragter, IT-Verantwortlicher
Verantwortlich für Umsetzung:	Brandschutzbeauftragter, Technische Abteilung

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

- **Sicherung mobiler Computer (M1.5)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Anwender

Bei der Speicherung von schützenswerten Daten auf mobilen Computern (Notebooks) sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Derartige Daten müssen verschlüsselt werden.
Notebooks sind möglichst verschlossen aufzubewahren.

2.1.3. Hard- und Software

- **Kontrollierter Softwareeinsatz (M1.6)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Anwender

Auf Rechnersystemen der Freien Universität Berlin darf zum Zweck des Schutzes von universitätseigener Hardware und dem Universitätsnetz nur Software installiert werden, die von der zuständigen Stelle dafür freigegeben wurde. Das eigenmächtige Einspielen oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn eine Erlaubnis oder eine pauschale Freigabe der zuständigen Stelle vorliegt.

- **Einsatz von privater Hard- und Software (M1.7)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Anwender

Der Einsatz von privater Hard- und Software im Bereich Forschung und Lehre richtet sich im Allgemeinen nach den fachbereichsinternen Regelungen. Bei Fehlen entsprechender Regelungen sollte nach Möglichkeit nur universitätseigene Hard- und Software eingesetzt werden. In speziell gekennzeichneten Bereichen, wie z.B. im Bereich des Wireless Lan der Freien Universität, ist der Einsatz von privater Hard- und Software erlaubt.

In besonders geschützten Bereichen und im Umgang mit Verwaltungsdaten, wie zum Beispiel alle personenbezogenen Daten der Beschäftigten und Studierenden und Daten der Ressourcenverwaltung, ist die Benutzung von priva-

ter Hard- und Software in Verbindung mit technischen Einrichtungen der Freien Universität Berlin und deren Netzen nicht gestattet. Sondergenehmigungen, zum Beispiel im Rahmen von Schulungsveranstaltungen oder Vorträgen, können auf Antrag durch die zuständigen IT-Verantwortlichen der Organisationseinheit oder dafür zuständiges IT-Personal erteilt werden.

- **Virenschutz (M1.8)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

Bei Verdacht auf Vireninfektion ist das zuständige IT-Personal zu informieren.

2.1.4. Zugriffsschutz

- **Abmelden und ausschalten (M1.9)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Bei kürzerem Verlassen des Zimmers, d.h. bis ca. 10 Minuten, muss der Arbeitsplatz-PC durch einen Kennwortschutz gesperrt werden. Bei längerem Verlassen des Zimmers muss sich der Benutzer aus den laufenden Anwendungen und dem Betriebssystem abmelden. Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen. (Beispielsweise kann die Rechenzeit von Arbeitsplatz-PCs in den Ruhephasen zu wissenschaftlichen Zwecken genutzt werden.)

- **Personenbezogene Kennungen (M1.10)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

- **Gebrauch von Passwörtern (M1.11)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Der Benutzer hat sein Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden.
Sofern die technischen Gegebenheiten dies zulassen, sind Passwörter nach den folgenden Regeln zu gestalten:

- Das Passwort muss mindestens 8 Stellen lang sein.
- Das Passwort muss mindestens einen Buchstaben und mindestens eine Ziffer oder ein Sonderzeichen enthalten.
- Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln und sollte eine Mindestgültigkeitsdauer von einem Tag haben.
- Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.

Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt.

Erhält ein Benutzer beim Anmelden mit seinem Passwort keinen Zugriff auf das System, besteht die Gefahr, dass sein Passwort durch Ausprobieren ermittelt wurde, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem zuständigen Vorgesetzten und dem IT-Personal zu melden. (Siehe M1.2)

Bei Vergessen des Passwortes bzw. nach mehrfacher fehlerhafter Passworteingabe hat der Benutzer die für diesen Fall vorgesehene Verfahrensweise zu befolgen. Die Zahl der erlaubten Fehlversuche wird von der zuständigen Stelle festgelegt. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird. In vielen Systemen muss das Zurücksetzen des Passworts durch den Administrator veranlasst werden. Andere Systeme sehen für diesen Fall vor, dass der Benutzer sich selbst wieder registriert.

- **Zugriffsrechte (M1.12)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal (bereichsspezifisch)

Der Benutzer darf nur mit den Zugriffsrechten ausgestattet werden, die unmittelbar für die Erledigung seiner Aufgaben vorgesehen sind.
Im Bereich der Universitätsverwaltung erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer auf schriftlichen Antrag.

In allen anderen Organisationseinheiten sind die dort geltenden Regelungen zu beachten.

- **Netzzugänge (M1.13)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Der Anschluss von Systemen an das Datennetz der Freien Universität Berlin hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems o. ä.) ist unzulässig. Ausnahmen dürfen nur die zuständigen FU-Rechenzentren in Absprache mit dem IT-Verantwortlichen der Organisationseinheit und ggf. mit dem Datenschutzbeauftragten einrichten.

2.1.5. Kommunikationssicherheit

- **Sichere Netzwerknutzung (M1.14)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Der Einsatz von verschlüsselten Kommunikationsdiensten ist, nach Möglichkeit, den unverschlüsselten Diensten vorzuziehen. Schützenswerte Daten sollten verschlüsselt übertragen werden.

2.1.6. Datensicherung

- **Datensicherung (M1.15)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen o. ä. schützen. Grundsätzlich sind Daten auf zentralen Servern zu speichern. Ist die Sicherung auf zentralen Servern noch nicht möglich, ist der Benutzer für die Sicherung seiner Daten selbst verantwortlich.

Den in den jeweiligen Organisationseinheiten geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung ist Folge zu leisten.

2.1.7. Umgang mit Datenträgern

- **Sichere Aufbewahrung (M1.16)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Mobile Datenträger mit schützenswerten Daten sind verschlossen und vor unbefugtem Zugriff geschützt aufzubewahren. Die Lagerungsbedingungen gemäß den Herstellerangaben sind einzuhalten. Insbesondere ist darauf zu achten, dass ein hinreichender Schutz gegen Hitze, Feuchtigkeit und magnetische Felder besteht.

- **Datenträgerkennzeichnung (M1.17)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

- **Gesicherter Transport (M1.18)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

- **Physisches Löschen von Datenträgern (M1.19)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Datenträger mit schützenswerten Daten müssen vor einer Weitergabe an nicht autorisierte Personen physisch gelöscht werden. Das kann mit geeigneten Programmen oder mit einem Gerät zum magnetischen Durchflutungslöschen erfolgen.

Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Vorzugsweise ist auch hier das Durchflutungslöschen und die daran anschließende mechanische Zerstörung anzuwenden.

Geeignete Werkzeuge und Anleitungen werden u. a. vom FU-Rechenzentrum bereitgestellt. Diese Aufgabe kann auch von geeigneten externen Dienstleistern erledigt werden.

2.1.8. Schützenswerte Daten

- **Schützenswerte Daten auf dem Arbeitsplatz-PC (M1.20)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

- **Sichere Entsorgung vertraulicher Papiere (M1.21)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Papiere mit vertraulichem Inhalt (einschließlich Testausdrucken) sind mit Hilfe eines Aktenvernichters zu vernichten. Alternativ kann die Entsorgung auch zentral über einen Dienstleister erfolgen. Bei der Entsorgung über einen Dienstleister sind die universitären Regelungen zu beachten.

2.2. Maßnahmen des IT-Grundschutzes für IT-Personal

Die im Folgenden beschriebenen Maßnahmen richten sich an alle Mitarbeiter der Freien Universität Berlin, die verantwortlich Aufgaben im Bereich des IT-Betriebs wahrnehmen oder Verantwortung im organisatorischen Bereich tragen. Insbesondere sind dies IT-Abteilungsleiter, IT-Verantwortliche, Verfahrensverantwortliche, System- und Netzadministratoren, Applikationsbetreuer, Benutzerservice, Programmentwickler u.a. Die im vorangegangenen Abschnitt dargestellten Maßnahmen für den IT-Anwender werden hier vorausgesetzt.

Im Interesse einer möglichst übersichtlichen Darstellung werden einige Maßnahmen wiederholt, wobei sie gelegentlich weiter ausgeführt oder erweitert werden. Bei spezifischen Aufgabenstellungen, insbesondere im Umfeld von System- und Netzadministration, kann eine Abweichung in einzelnen Punkten der zuvor behandelten Maßnahmen notwendig sein. In jedem Fall ist aber der zugrunde liegende Sicherheitsgedanke nicht außer Kraft zu setzen, sondern der gegebenen Situation anzupassen.

2.2.1. Allgemeines

- **Grundsätze für den IT-Einsatz (M2.1)**

Verantwortlich für Initiierung:	Universitätsleitung (CIO-Gremium)
Verantwortlich für Umsetzung:	Bereichsleitung, IT-Verantwortlicher

Beschaffung, Entwicklung und Einsatz von IT-Anwendungen und -Systemen erfolgt nach Maßgabe der für die Universität geltenden Regelungen. Zusätzlich sind Regelungen des Bundes und des Landes Berlin zu beachten, die eine ordnungsgemäße IT-Organisation, Verfahrensplanung und -realisierung beschreiben, soweit diese für die Freie Universität Berlin verbindlich sind.

- **Gesamtverantwortung (M2.2)**

Verantwortlich für Initiierung:	Universitätsleitung (CIO-Gremium)
Verantwortlich für Umsetzung:	Bereichsleitung

Die Verantwortung für die Umsetzung und Einhaltung der für den IT-Einsatz geltenden Regelungen tragen die einzelnen Bereichsleitungen (Dekanate, Leitungen) in den Fachbereichen, Zentraleinrichtungen und -instituten und der Zentralen Universitätsverwaltung entsprechend den Regelungen des Berliner Hochschulgesetzes.

2.2.2. Organisation von IT-Sicherheit

- **Beschreibung von IT-Verfahren (M2.3)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	Verfahrensverantwortlicher

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

- **Rollentrennung (M2.4)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

- **Benennung eines IT-Verantwortlichen (M2.5)**

Verantwortlich für Initiierung:	Universitätsleitung (CIO-Gremium)
Verantwortlich für Umsetzung:	Bereichsleitung

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

Eine nähere Beschreibung von Rolle und Aufgaben des IT-Verantwortlichen ist in der IT-Organisationsrichtlinie enthalten.

- **Dokumentation der IT-Verfahren bezüglich der IT-Sicherheit (M2.6)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

IT-Verfahren sind bezüglich der Sicherheit mindestens hinsichtlich der folgenden Punkte zu dokumentieren:

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

Darüber hinaus sind die Regelungen der bestehenden IT-Rahmendienstvereinbarung zur Dokumentation von IT-Verfahren zu beachten. Nur dokumentierte Verfahren dürfen betrieben werden. Der IT-Verantwortliche sorgt für die aktuelle Dokumentation der Verfahren seiner Organisationseinheit. Der IT-Verantwortliche ist verantwortlich für die Erstellung und Pflege der Doku-

mentation der Verfahren seiner Organisationseinheit. Verfahrensverantwortliche, Systemadministratoren und Applikationsbetreuer sind dabei durch die IT-Organisationsrichtlinie zur Mitarbeit verpflichtet.

- **Dokumentation von Ereignissen und Fehlern (M2.7)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

- **Regelungen der Auftragsdatenverarbeitung (M2.8)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	Verfahrensverantwortlicher

Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag der Freien Universität Berlin betriebenen IT-Verfahren. Es sind eindeutige Zuweisungen der Verantwortlichkeit für die IT-Sicherheit zu schaffen und entsprechende Kontrollmöglichkeiten vorzusehen.

Sofern im Rahmen der Auftragsdatenverarbeitung personenbezogene Daten verarbeitet werden, sind die entsprechenden Regelungen des Berliner Datenschutzgesetzes zu beachten. Für Wartungsarbeiten stellt das Berliner Datenschutzgesetz besondere Regelungen bereit, die anzuwenden sind.

- **Standards für technische Ausstattung (M2.9)**

Verantwortlich für Initiierung:	Universitätsleitung (CIO-Gremium)
Verantwortlich für Umsetzung:	IT-Dienstleister

Zur Erreichung eines ausreichenden Sicherheitsniveaus für IT-Systeme sind Qualitätsstandards im Sinne dieser Richtlinie von den zentralen Dienstleistern unter Maßgabe der vom CIO-Gremium definierten Strategien zu formulieren und regelmäßig neuen Anforderungen anzupassen. Bei der Entwicklung der Standards sind die spezifischen Bedürfnisse der Fachbereiche zu berücksichtigen.

- **Zentralisierung wichtiger Serviceleistungen (M2.10)**

Verantwortlich für Initiierung:	Universitätsleitung (CIO-Gremium), Bereichsleitung
Verantwortlich für Umsetzung:	IT-Dienstleister, IT-Verantwortlicher, IT-Personal

Ein leistungsfähiger Nutzerservice, zentral gesteuerte Datensicherungsmaßnahmen, die Möglichkeit der Ablage von Daten auf zentralen Fileservern sowie die Möglichkeit der Ausführung von Programmen auf Applikationsservern sind wesentliche Voraussetzungen für einen sicheren und reibungslosen IT-Einsatz zur Unterstützung der täglichen Arbeitsprozesse. Die Softwareverteilung inkl. -installation und -inventarisierung sollte mit Unterstützung entsprechender Werkzeuge erfolgen. Maßnahmen zur Virenabwehr sind ebenfalls zu zentralisieren.

Beim Einsatz netzwerkweit operierender Installations- und Inventarisierungswerkzeuge sind besondere Maßnahmen zum Schutz vor Missbrauch zu ergreifen. Insbesondere müssen verbindliche Regelungen getroffen werden, die sicherstellen, dass die Werkzeuge ausschließlich für diesen Zweck eingesetzt werden. Dazu muss u. a. festgelegt sein, dass die Werkzeuge nur auf dafür bestimmten, besonders abgesicherten Arbeitsplätzen eingesetzt werden. Der Personenkreis, der berechtigt ist, diese Werkzeuge zu nutzen, ist auf das notwendige Maß zu beschränken. Die Anwender sind vor dem Einsatz solcher Werkzeuge zu informieren. Ihr Einsatz muss protokolliert und dokumentiert werden.

- **Revision der Sicherheit (M2.11)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Alle eingerichteten Sicherheitsvorkehrungen müssen auf ihre Tauglichkeit und auf unerlaubte Veränderungen hin überprüft werden. Diese Überprüfung muss regelmäßig und nach jeder Änderung der Sicherheitsstandards erfolgen. Dies kann mit Hilfe entsprechender Tools von den zuständigen IT-Stellen der Freien Universität Berlin selbst oder durch externe Dienstleister durchgeführt werden. Bei der Vergabe dieser Tätigkeit an externe Auftragnehmer ist auf deren Seriosität besonderen Wert zu legen. (Zum Beispiel wäre es sinnvoll, nur Anbieter mit Zertifikaten des BSI in Betracht zu ziehen.)

- **Allgemeine Notfallvorsorge (M2.12)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Bei der Einführung neuer IT-Verfahren bzw. neuer IT-Arbeitsprozesse werden im Rahmen der Dokumentationspflichten Analysen zur Ermittlung des Schutzbedarfs und ggf. zur Identifizierung und Begegnung spezifischer Risiken vorgenommen. Basierend auf den Ergebnissen dieser Analysen sollte ein Notfallplan erstellt werden, in dem festgelegt wird, wie auf Notfallsituationen adäquat reagiert wird. „Notfall“ bezeichnet eine Situation, in der durch eine Betriebsstö-

rung die Verfügbarkeit, Integrität oder Vertraulichkeit der Daten nicht mehr gegeben ist und ein verhältnismäßig hoher Schaden entsteht. In einem Notfallplan sollten zum Beispiel Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten und zum Einsatz von Ausweichmöglichkeiten enthalten sein. Darüber hinaus ist es häufig sinnvoll einen Alarmierungsplan zu erstellen, in dem die Meldewege im Notfall beschrieben sind.

2.2.3. Personelle Maßnahmen

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

- **Sorgfältige Personalauswahl (M2.13)**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	Bereichsleitung

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

- **Angemessene Personalausstattung (M2.14)**

Verantwortlich für Initiierung:	Bereichsleitung (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Bereichsleitung

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

- **Vertretung (M2.15)**

Verantwortlich für Initiierung:	Bereichsleitung (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
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 und nach Möglichkeit auch technisch festgelegt sein und darf nicht durch die Weitergabe von Passwörtern erfolgen.

Die technischen Voraussetzungen für die Wahrnehmung einer Vertretung sollten möglichst ständig eingerichtet sein. Eine Ausnahme bilden systemspezifische, nicht nutzerabhängige Kennungen (zum Beispiel *root* bei UNIX-Systemen). Dort soll der Vertreter nur im Bedarfsfall auf das an geeigneter Stelle hinterlegte Passwort des Administrators zurückgreifen können.

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

- **Qualifizierung (M2.16)**

Verantwortlich für Initiierung:	Bereichsleitung (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Bereichsleitung

IT-Personal darf erst nach ausreichender Schulung mit IT-Verfahren/IT-Arbeitsprozessen arbeiten. Dabei sind ihnen die für sie geltenden Sicherheitsmaßnahmen, die rechtlichen Rahmenbedingungen sowie ggf. die Erfordernisse des Datenschutzes zu erläutern. Es muss sichergestellt sein, dass die ständige Fortbildung des IT-Personals in allen ihr Aufgabengebiet betreffenden Belangen erfolgt.

2.2.4. Sicherung der Infrastruktur

- **Sicherung der Serverräume (M2.17)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	Technische Abteilung

Alle Rechnersysteme mit typischer Serverfunktion, einschließlich der Peripheriegeräte (Konsolen, externe Platten, Laufwerke u. ä.), sind in separaten, besonders gesicherten Räumen aufzustellen. Der Zugang Unbefugter zu diesen Räumen muss zuverlässig verhindert werden. 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, einbruchsichere Türen, Bewegungsmelder o. ä. zur Verhinderung eines gewaltsamen Eindringens vorzusehen.

Serverräume, in denen besonders schützenswerte Daten gespeichert bzw. verarbeitet werden und die nicht über entsprechende bauliche Sicherungsvorkehrungen verfügen, sollen möglichst unauffällig sein, d. h. Hinweisschilder u. ä. sollten nicht angebracht werden, damit die Funktion der Räume nicht sofort erkennbar wird. Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; verwendete Schlüssel müssen kopiergeschützt sein. Für die Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen. Der Zutritt muss auf diejenigen Personen begrenzt werden, deren Arbeitsaufgaben dieses erfordern. Das Betreten der Räume darf nur nach vorheriger Anmeldung

bei der für die Räume verantwortlichen Stelle erfolgen. Reinigungspersonal soll die Serverräume nach Möglichkeit nur unter Aufsicht betreten.

- **Geschützte Aufstellung von Endgeräten (M2.18)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Verantwortlicher

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

- **Umgang mit Schutzschränken (M2.19)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Bei der Aufstellung von Schutzschränken ist das in der Regel hohe Gewicht zu beachten und daher die ausreichende Tragfähigkeit des Fußbodens sicher zu stellen. Schutzschränke mit geringer Größe bzw. geringem Gewicht sollten so verankert werden, dass der Diebstahlschutz gewährleistet ist. Außerdem sind eventuell vorhandene Herstellerhinweise, z.B. zu notwendigen freien Lüftungsöffnungen, zu beachten. Generell sind Schutzschränke bei Nichtbenutzung verschlossen zu halten.

- **Sicherung der Netzknoten (M2.20)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Dienstleister

Vernetzungsinfrastruktur (Switches, Router, Hubs, Wiring-Center u. ä.) ist grundsätzlich in verschlossenen Räumen oder in nicht öffentlich zugänglichen Bereichen in verschlossenen Schränken einzurichten, die gegen unbefugten Zutritt und Zerstörung ausreichend gesichert sind. Es gelten die gleichen Empfehlungen wie unter M2.17.

- **Verkabelung und Funknetze (M2.21)**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	IT-Dienstleister

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

deaktiviert werden. Erweiterungen und Veränderungen an der Gebäudeverkabelung, auch die Inbetriebnahme von Funknetzen, sind mit den IT-Verantwortlichen der eigenen Organisationseinheit und mit dem Hochschulrechenzentrum abzustimmen.

- **Geschützte Kabelverlegung (M2.22)**

Verantwortlich für Initiierung:	Universitätsleitung (CIO-Gremium)
Verantwortlich für Umsetzung:	IT-Dienstleister

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.

- **Einweisung und Beaufsichtigung von Fremdpersonal (M2.23)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	Universitäts-/Bereichsleitung, IT-Verantwortlicher

Fremde Personen, die in gesicherten Räumen mit IT (z.B. Serverräume) Arbeiten auszuführen haben, müssen beaufsichtigt werden. Personen, die nicht unmittelbar zum IT-Bereich zu zählen sind, aber Zugang zu gesicherten IT-Räumen benötigen, müssen über den Umgang mit IT belehrt werden.

Wenn bei Arbeiten durch externe Firmen, zum Beispiel im Rahmen der Fernwartung, die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, müssen diese Personen gemäß §8 des Berliner Datenschutzgesetzes auf das Datengeheimnis verpflichtet sein. Für die Wartung und Instandhaltung sind Verträge gemäß §3a Berliner Datenschutzgesetz zu schließen.

Alle Aktionen, die von externen Firmen durchgeführt werden, sollten nach Möglichkeit überwacht und protokolliert werden.

- **Stromversorgung und Überspannungsschutz (M2.24)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Dienstleister, IT-Personal

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. Bei Einsatz von Geräten mit redundant ausgelegter Stromversorgung ist darauf zu achten, dass die einzelnen Netzteile über getrennt abgesicherte Stromkreise versorgt werden. Die für den Betrieb von IT notwendigen Unterlagen und Informationen zur elektrischen Versorgung sind dem IT-Verantwortlichen auf Anfrage von den IT-Dienstleistern bzw. der Technischen Abteilung zur Verfügung zu stellen.

- **USV (M2.25)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Dienstleister, IT-Personal

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

- **Brandschutz (M2.26)**

Verantwortlich für Initiierung:	IT-Verantwortlicher Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Technische Abteilung

Die Regeln des vorbeugenden Brandschutzes sind zu beachten und einzuhalten. Insbesondere gilt dies für Räume mit wichtiger Informationstechnik, wie beispielsweise Serverräume. Papierlager, leere Verpackungen und andere leicht entflammbare Materialen dürfen in diesen Räumen nicht gelagert werden. In diesen Räumen sowie in anderen Technikräumen besteht Rauchverbot. Die Türen zu diesen Räumen sollen brandhemmend ausgelegt sein. In diesem Zusammenhang sind die Schutzklassen T30 und T90 zu nennen. Außerdem sind Brandmelder und Handfeuerlöscher (Brandklasse B, CO_2-Löscher) vorzusehen. Für Hinweise und eingehende Beratung wenden Sie sich an Ihren örtlichen Brandschutzbeauftragten.

- **Schutz vor Wasserschäden (M2.27)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
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. 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.

- **Klimatisierung (M2.28)**

Verantwortlich für Initiierung:	IT-Verantwortlicher, Bereichsleitung (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
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 Raumes gestellt werden. Die Gewährleistung der zulässigen IT-Betriebstemperatur und demzufolge die Sicherstellung des IT-Betriebs steht in engem Zusammenhang mit dem reibungslosen Einsatz von Klimatisierungsgeräten. Daher müssen die Geräte mit einer hohen Verfügbarkeit ausgestattet sein.

Klimatisierungsanlagen sind an geeigneter Stelle aufzustellen und regelmäßig zu warten. In klimatisierten Räumen, die ständig mit Personal besetzt sind, ist eine Frischluft-Beimischung notwendig.

2.2.5. Hard- und Softwareeinsatz

- **Beschaffung, Softwareentwicklung (M2.29)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Verantwortlicher

Die Beschaffung von Soft- und Hardware ist mit dem zuständigen IT-Verantwortlichen abzustimmen. Dieser ist für die Einhaltung von Standards und Sicherheitsanforderungen verantwortlich.

Bei der Entwicklung von Software müssen vorher die fachlichen und technischen Anforderungen spezifiziert sein. Diese Arbeiten werden in enger Abstimmung mit den betroffenen Organisationseinheiten durchgeführt.

- **Kontrollierter Softwareeinsatz (M2.30)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Auf Rechnersystemen der Freien Universität Berlin darf zum Zweck des Schutzes von universitätseigener Hardware und dem Universitätsnetz 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, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn eine Genehmigung der zuständigen Stelle vorliegt oder eine Organisationseinheit eine pauschale Freigabe für Teilbereiche festgelegt hat. Rechnersysteme sind gegen das unbefugte Herunterladen hard- und softwaretechnisch zu schützen.

- **Separate Entwicklungsumgebung (M2.31)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

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

- **Test von Software (M2.32)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Vor dem Einsatz neuer Software oder neuer Versionen muss die Erfüllung der Spezifikation durch hinreichende Tests sichergestellt sein. Der Testverlauf und das Testergebnis sind zu dokumentieren.

- **Entwicklung von Software nach standardisierten Verfahren (M2.33)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Softwareentwicklungen, die auf Grund ihrer Größenordnung Projektcharakter haben, müssen nach standardisierten Verfahren (Vorgehensmodelle) und nach Maßgabe der für die Universität geltenden Regelungen (u. a. ein klar umrissenes Projektmanagement und eine Qualitätssicherung) durchgeführt werden.

- **Schutz vor Schadprogrammen (M2.34)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Auf allen Arbeitsplatz-PCs ist, soweit möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Jede Organisationseinheit ist verpflichtet, Virenschutzsysteme anzubieten. Durch den Einsatz von Virenschutzsystemen soll das Eindringen von schädlichem Programmcode erkannt und verhindert werden. Regelmäßig (möglichst automatisiert) sind die Virenerkennungsmuster zu aktualisieren. Wird auf einem System schädlicher Programmcode entdeckt, muss dies der zuständigen Stelle gemeldet und das Ergebnis der eingeleiteten Maßnahmen dokumentiert werden.

Empfehlenswert ist, in regelmäßigen Abständen sowie bei konkretem Bedarf oder Verdacht eine Suche nach Schadprogrammen auf allen bedrohten IT-Systemen vorzunehmen und die Ergebnisse zu dokumentieren.

- **Kontrollierte PC-Schnittstellen (M2.35)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

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

- **Dokumentation (M2.36)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

Zu jedem IT-System ist eine Dokumentation zu führen. Üblicherweise werden nicht einzelne PCs gesondert dokumentiert, sondern zu größeren Gruppen zusammengefasst. Die Dokumentation muss mindestens den Aufstellungsort und Unterlagen zur Hard- und Softwareausstattung, Garantieleistungen, Wartungsverträgen, Lizenzen usw. enthalten. Darüber hinaus sind Angaben zur Hard- und Softwarekonfiguration, zu durchgeführten Reparaturarbeiten, aufgetretenen Problemen, Suche nach Schadprogrammen und zur Verantwortlichkeit zu dokumentieren. Regelungen zur Datensicherung (Umfang, Verfahren, Rhythmus usw.) sind ebenfalls zu dokumentieren.

- **Ausfallsicherheit (M2.37)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Dienstleister, IT-Personal

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

- **Einsatz von mobilen PCs (M2.38)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Mobile PCs können typischerweise sowohl mobil als auch stationär genutzt werden und damit auch auf unterschiedliche Netze zugreifen. Daraus resultiert, dass bei der mobilen Nutzung die Daten auf dem mobilen PC gegen Verlust, Manipulation und unberechtigte Einsichtnahme geschützt werden müssen. Andererseits muss sichergestellt werden, dass keine Gefährdungen von mobilen PCs auf andere IT-Systeme und Netze ausgehen können.

Bei der Nutzung von mobilen PCs durch verschiedene Personen muss die Übergabe geregelt stattfinden. Dabei muss mindestens nachvollziehbar sein, wo sich das Gerät befindet und welche Person das Gerät benutzt.

- **Einsatz von Diebstahl-Sicherungen (M2.39)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Technische Abteilung, IT-Personal

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen – z. B. geeignete Zutrittskontrolle zu den Arbeitsplätzen – nicht umgesetzt werden können. Diebstahl-Sicherungen machen z. B. dort Sinn, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Mit Diebstahl-Sicherungen sollten je nach zu schützendem Objekt nicht nur das IT-System selber, sondern auch Monitor, Tastatur und anderes Zubehör ausgestattet werden.

2.2.6. Zugriffsschutz

Grundsätzlich gilt, dass nur die Personen Zugang zu dem Netz und den damit verfügbaren Ressourcen der Freien Universität Berlin erhalten, die zuvor die Erlaubnis zur Nutzung von den dafür zuständigen Stellen erhalten haben. Jede Nutzungserlaubnis muss personengebunden sein, d.h. anonyme Nutzerkonten sollten nur in begründeten Ausnahmefällen (beispielsweise als Zugang für FTP- oder WWW-Server) erlaubt werden. Die Verwendung fremder Nutzerkennungen ist nicht erlaubt.

In der Regel ist der Zugang zum Netz verbunden mit dem Zugriff auf Daten, Anwendungsprogramme und weitere Ressourcen. Daher hat die Authentisierung der Nutzer des Netzes an jedem einzelnen Arbeitsplatz-PC der Universität eine besondere Bedeutung.

- **Bereitstellung von Verschlüsselungssystemen (M2.40)**

Verantwortlich für Initiierung:	Universitätsleitung (CIO-Gremium)
Verantwortlich für Umsetzung:	IT-Dienstleister

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

- **Netzzugänge (M2.41)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Der Anschluss von Systemen an das Datennetz der Freien Universität Berlin hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems o.ä.) ohne Absprache mit dem IT-Verantwortlichen der Organisationseinheit und ggf. mit dem Datenschutzbeauftragten ist unzulässig.

- **Personenbezogene Kennungen (Authentisierung) (M2.42)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

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 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, Kennungen und Passwörter weiterzugeben.

Redundanzen bei der Benutzerverwaltung sind zu vermeiden. Die Zuordnung von mehreren Kennungen zu einer Person innerhalb eines IT-Systems sollte nur in begründeten Ausnahmefällen erlaubt sein, wie beispielsweise für Systemadministratoren. Die Einrichtung und Freigabe einer Benutzerkennung dürfen nur in einem bereichsintern geregelten Verfahren erfolgen. Die Einrichtung und Freigabe sind zu dokumentieren.

- **Administratorkennungen (M2.43)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

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

- **Ausscheiden von Mitarbeitern (M2.44)**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	Bereichsleitung, Vorgesetzter des ausscheidenden Mitarbeiters

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass der zuständige IT-Verantwortliche bzw. Verfahrensverantwortliche rechtzeitig über das Ausscheiden oder den Wechsel eines Mitarbeiters informiert wird. Die zuständige Organisationseinheit des betreffenden Mitarbeiters hat über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung des ausscheidenden Mitarbeiters zugeordnet sind. Vor dem Ausscheiden sind sämtliche Unterlagen, die sicherheitsrelevante Angaben enthalten sowie ausgehändigte Schlüssel zurück zu fordern. Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt, so ist nach dem Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.

- **Passwörter (M2.45)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal , IT-Anwender

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

  - Das Passwort darf nicht leicht zu erraten sein, wie Namen, Kfz-Kennzeichen, Geburtsdatum.
  - Das Passwort muss mindestens einen Buchstaben und mindestens eine Ziffer oder ein Sonderzeichen enthalten.

- Das Passwort sollte mindestens 8 Zeichen lang sein. Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.
- Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.
- Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes muss unbeobachtet stattfinden.

Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern ("BBBBBB", "123456") sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpasswörtern.
- Nach mehrfacher fehlerhafter Passworteingabe muss eine Sperrung erfolgen, die entweder vom Systemadministrator, durch erneute Selbstregistrierung oder nach Ablauf einer Sperrfrist automatisch aufgehoben wird.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

- Die Passwörter sollten im System zugriffssicher gespeichert werden, z. B. mittels Einwegverschlüsselung.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).

Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt.

- **Zugriffsrechte (Autorisierung) (M2.46)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

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

Im Bereich der Universitätsverwaltung erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer auf schriftlichen Antrag. In allen anderen Organisationseinheiten sind die dort geltenden Regelungen zu beachten.

Es ist zu prüfen, inwieweit die Zugriffserlaubnis auf bestimmte Arbeitsplatz-PCs begrenzt werden kann. Für Benutzer mit besonderen Rechten, insbesondere für Administratorkennungen, ist eine Zugriffserlaubnis auf die notwendigen Rechner (i.d.R. sind es der betreffende Server und die Arbeitsplatz-PCs) zu begrenzen. Es ist ebenfalls zu prüfen, inwieweit die Zugangserlaubnis auf bestimmte Zeiten begrenzt werden kann. Beispielsweise könnte der Zugang zu wichtigen Systemen für die Anwender auf die üblichen Arbeitszeiten eingeschränkt werden.

- **Änderung der Zugriffsrechte (M2.47)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

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, um die Berechtigungsänderungen im System abzubilden.

- **Abmelden und ausschalten (M2.48)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal , IT-Anwender

Bei kürzerem Verlassen des Raumes, d.h. bis ca. 10 Minuten, muss der Zugriff auf das IT-System durch einen Kennwortschutz gesperrt werden. Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen. (Beispielsweise kann die Rechenzeit von Arbeitsplatz-PCs in den Ruhephasen zu wissenschaftlichen Zwecken genutzt werden.) Soweit es technisch möglich ist, sollte ein Arbeitsplatz-PC so konfiguriert sein, dass nach längerer Inaktivität (beispielsweise 20 Minuten) der PC automatisch gesperrt wird und nur nach erneuter Eingabe eines Passwortes zu aktivieren ist.

2.2.7. System- und Netzwerkmanagement

Eine angemessene Protokollierung, Audit und Revision sind wesentliche Faktoren der Netzsicherheit. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt, oder die Erkennung von systematischen Angriffen auf das Netz.

Unter einem Audit wird die Verwendung eines Dienstes verstanden, der insbesondere sicherheitskritische Ereignisse betrachtet. Bei einem Audit werden die Ereignisse mit Hilfe geeigneter Werkzeuge betrachtet und ausgewertet.

Protokolle dienen dem Erkennen und Beheben von Fehlern. Mit ihrer Hilfe lässt sich feststellen, wer wann welche Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Für die Verarbeitung personenbezogener Daten ist dies gesetzlich vorgeschrieben (§ 5 Abs. 2 Nr. 5 BlnDSG).

Je nach Schutzbedarf des Verfahrens müssen adäquate Maßnahmen zur Protokollierung getroffen werden, um die Revisionsfähigkeit zu gewährleisten.

Bei der Revision werden die beim (Offline-) Audit gesammelten Daten von einem oder mehreren unabhängigen Mitarbeitern (4-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken und die Arbeit der Administratoren zu kontrollieren.

- **Protokollierung durch Betriebssysteme (M2.49)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

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

Die Protokolle sollten regelmäßig und zeitnah ausgewertet werden. Es muss dabei sicher gestellt sein, dass nur die Personen Zugriff auf die Protokolle erlangen können, die dafür von der zuständigen Stelle mit den nötigen Rechten ausgestattet wurden. Das Prinzip der Zweckbindung nach § 11 Abs. 5 BlnDSG ist unbedingt zu beachten.

- **Protokollierung durch Anwendungsprogramme (M2.50)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

Bei der Protokollierung durch Anwendungsprogramme ist der Grundsatz der Datenvermeidung § 5a BlnDSG zu beachten, d.h. es sind so wenig personenbezogene Daten wie möglich zu protokollieren. Von Anwendungsprogrammen erzeugte Protokolldaten sind vor dem Zugriff Unbefugter zu schützen. Es gelten die oben genannten Regeln (M 2.46) entsprechend, insbesondere ist bei Daten mit Personenbezug das Zweckbindungsgebot § 11 Abs. 5 BlnDSG zu beachten.

- **Protokollierung der Administrationstätigkeit (M 2.51)**

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Personal

Die Administratoren sind durch organisatorische Regelungen (Dienstanweisungen o.ä.) je nach Schutzbedarf des Verfahrens bzw. der zu verarbeitenden Daten zu verpflichten, die im Rahmen ihrer Aufgaben durchgeführten Tätigkeiten zu protokollieren.

2.2.8. Kommunikationssicherheit

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. Alle IT-Nutzer der Universität sind über die besonderen Risken und Gefahren der elektronischen Kommunikation und der Datenübermittlung in Kenntnis zu setzen.

- **Sichere Netzwerkadministration (M2.52)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister

Es muss geregelt und sichergestellt sein, dass die Administration des lokalen Netzwerks nur von dem dafür vorgesehenen Personal durchgeführt wird. Aktive und passive Netzkomponenten sowie Server sind vor dem Zugriff Unbefugter zu schützen.

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

- **Netzmonitoring (M2.53)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister

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

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

- **Deaktivierung nicht benötigter Netzwerkzugänge (M2.54)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister

Es sind alle nicht benötigten Netzwerkzugänge zu deaktivieren, damit ein unbefugter Zugang zum Netz der Freien Universität Berlin verhindert wird.

- **Kommunikation zwischen unterschiedlichen Sicherheitsniveaus (M2.55)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister

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 (z.B. der Betrieb eines Modems zu Fernwartungszwecken), muss dies zuvor durch die zuständige Stelle genehmigt werden. Jeder Zugriff Externer ist zu protokollieren.

2.2.9. Datensicherung

- **Organisation der Datensicherung (M2.56)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

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

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

- **Anwenderinformation zur Datensicherung (M2.57)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Alle Anwender, die prinzipiell Datensicherungssysteme nutzen können, sollten über die Regelung zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (z.B. ungeeignetes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können.

- **Durchführung der Datensicherung (M2.58)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Vorzugsweise sollten Daten auf zentralen Fileservern gespeichert werden. Dort erfolgt turnusmäßig eine zentrale Datensicherung. Wo ein Zugriff auf einen Fileserver derzeit noch nicht möglich ist, müssen die Daten lokal gesichert werden.

Für Daten, deren Wiederherstellung mehr als einige Tage erfordert, sind mindestens 3 Generationen von Sicherungen vorzuhalten. Es ist empfehlenswert, jeweils eine Sicherung für mindestens 3 bis 6 Monate aufzubewahren.

- **Durchführung der Datensicherung auf Servern (M2.59)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Die Sicherung der Daten auf Servern sollte im angemessenen Rhythmus erfolgen. Auch System- und Programmdaten sind nach Veränderungen zu si-

chern. Zur Datensicherung sind dafür geeignete Backup-Werkzeuge zu verwenden, die eine Datensicherung für Daten, deren Wiederherstellung mehr als einige Tage erfordert, nach dem Generationenprinzip unterstützen.

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

- **Verifizierung der Datensicherung (M2.60)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
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.

2.2.10. Datenträgerkontrolle

- **Aufbewahrung (M2.61)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
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 Tresor aufzubewahren (Schutzklasse mind. S 60 D, derartige Tresore sind entsprechend gekennzeichnet).

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, dass für die verwendeten Datenformate geeignet ist.

- **Datenträgerkennzeichnung und -inventarisierung (M2.62)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Alle mobilen Datenträger sind soweit möglich eindeutig zu kennzeichnen. Aus der Beschriftung soll die Verwendung (Verfahren, Dateien, Inhalt), Datum der ersten Ingebrauchnahme sowie das Datum des letztmaligen Beschreibens hervorgehen. In der zuständigen Stelle ist ein Verzeichnis aller verwendeten Datenträger zu führen. Dieses Verzeichnis muss stets aktuell gehalten werden.

- **Weitergabe von Datenträgern (M2.63)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

Die Weitergabe von Datenträgern darf nur an befugte Personen erfolgen. Befugt ist eine Person dann, wenn die Weitergabe der Datenträger im Verfahren vorgesehen ist. Die Weitergabe vertraulicher oder personenbezogener Daten auf Datenträgern darf nur gegen Quittung erfolgen.

- **Gesicherter Transport (M2.64)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal

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

- **Physisches Löschen und Entsorgung von Datenträgern (M2.65)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Wenn Datenträger, auf denen schützenswerte Daten gespeichert sind, zur weiteren Verwendung an Dritte gehen, müssen alle Daten vor der Weitergabe physisch gelöscht werden. Das kann mit geeigneten Programmen oder mit einem Gerät zum magnetischen Durchflutungslöschen erfolgen. Die von den Betriebssystemen dafür vorgesehenen Programme genügen in der Regel nicht. Bei Disketten kann ersatzweise auch ein mehrfaches Formatieren (mindestens dreimal) erfolgen. Eine Weitergabe an universitätsfremde Personen ist untersagt.

Auszusondernde oder defekte Datenträger müssen, sofern sie personenbezogene oder vertrauliche Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden. Vorzugsweise ist auch hier das Durchflutungslöschen und die mechanische Zerstörung anzuwenden (bei Disketten ersatzweise ein dreifaches Formatieren mit nachfolgender mechanischer Zerstörung).

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.

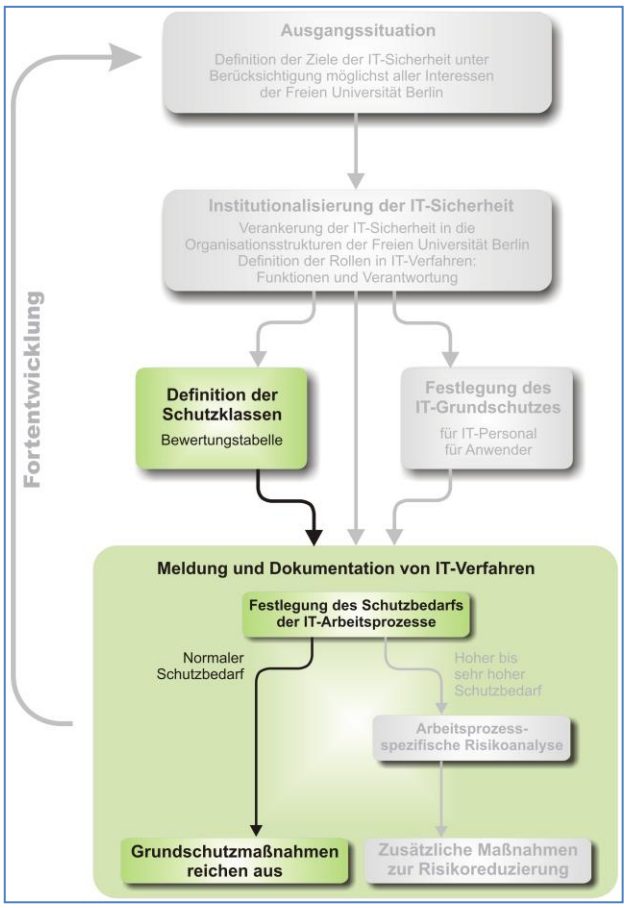
Die Reparatur beschädigter Datenträger, auf denen schützenswerte Daten gespeichert sind, ist nur in besonderen Ausnahmenfällen erlaubt. Wenn unter besonderen Umständen Datenträger durch externe Dienstleister repariert werden sollen, ist der Auftragnehmer auf die Wahrung der Vertraulichkeit der Daten zu verpflichten. Die Verpflichtung muss vertraglich verankert sein.

- **Sichere Entsorgung vertraulicher Papiere (M2.66)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

Papiere mit vertraulichem Inhalt sind mit Hilfe eines Aktenvernichters zu vernichten. Bei der Beschaffung eines Aktenvernichters ist die DIN 32757 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.

3. 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 Technik selbst. Daher sind IT-Sicherheitsmaßnahmen aus den Sicherheitsanforderungen der IT-Verfahren bzw. IT-Arbeitsprozesse abzuleiten.

Die Untersuchung eines IT-Verfahrens bzw. eines IT-Arbeitsprozesses hat daher mit der Analyse seines Schutzbedarfes zu beginnen. Die an der Freien Universität Berlin geltenden Regelungen zur Ermittlung des jeweils passenden Schutzbedarfes wurden in Anlehnung an das IT-Sicherheitshandbuch des BSI und an die einschlägigen Empfehlungen der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) aufgestellt und abgestimmt (Tabelle 1: Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren).

Der Bewertungsmaßstab klassifiziert den Schutzbedarf in drei Werte (Schutzklassen) „normal“, „hoch“ und „sehr hoch“ und beschreibt die Bedeutung dieser Werte in Hinblick auf verschiedene Kriterien. Für jedes IT-Verfahren bzw. jeden IT-Arbeitsprozess ist ein Mindestmaß an Sicherheit zu gewährleisten, daher sind die Regeln des IT-Grundschutzes (Kapitel 2 „Definition des Grundschutzes“) in allen IT-Verfahren/IT-Arbeitsprozesse verpflichtend einzuhalten. Aufgrund des Ergebnisses der Schutzbedarfsanalyse können sich weitere Anforderungen ergeben.

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

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

Beeinträchtigungen (Kategorien)	Verlust von	Bedrohung	Abschätzung des Schadens		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Vertr.	Bekannt werden der Daten für Unberechtigte ...	... würde durch den Einzelnen als tolerable Beeinträchtigung des informationellen Selbstbestimmungsrechts eingeschätzt werden. Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.	… führt möglicherweise zu einer erheblichen Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.	... führt möglicherweise zu einer bedeutenden Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
	Integ.	Unberechtigte Manipulation der Daten ...			
	Verfg.	Verlust der Daten ...			
Verstoß gegen Gesetze, Vorschriften und Verträge	Vertr.	Bekannt werden der Daten für Unberechtigte ...	... verstößt gegen Gesetze oder Vorschriften mit geringen Konsequenzen. … hat geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen zur Folge.	... verstößt gegen Gesetze oder Vorschriften mit erheblichen Konsequenzen. … hat Vertragsverletzungen mit hohen Konventionalstrafen und / oder erheblichen Haftungsschäden zur Folge.	... verstößt fundamental gegen Gesetze oder Vorschriften. … hat Vertragsverletzungen zur Folge, deren Haftungsschäden für die FU ruinös sind.
	Integ.	Unberechtigte Manipulation der Daten ...			
	Verfg.	Verlust der Daten ...			
Beeinträchtigung der persönlichen Unversehrtheit	Vertr.	Missbrauch der Daten ...	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen Unversehrtheit	... führt zu erheblicher Beeinträchtigung der persönlichen Unversehrtheit	... bedroht die Existenz des Betroffenen
	Integ.	Unberechtigte Manipulation der Daten ...			
	Verfg.	Verlust der Daten ...			
Beeinträchtigung der Aufgabenerfüllung	Vertr.	Die Kenntnisnahme der Daten durch Unbefugte ...	... würde von den Betroffenen als tolerabel eingeschätzt werden. Die Daten sind öffentlich oder im Rahmen des Dienstbetriebs sachlich zuständigen Bearbeitern zugänglich.	... würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt werden. Die Daten sind vertraulich mit erheblichem Wert für die Universität.	... würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die Daten unterliegen besonderer Geheimhaltung.
	Integ.	Unberechtigte Manipulation der Daten ...	... führt maximal zum Ausfall einzelner verwaltungstechnischer oder wissenschaftlicher Arbeitsabläufe	... schränkt die Auftragserfüllung in einem Teilbereich ein	... gefährdet den Auftrag der gesamten Universität
	Verfg.	Verlust der Daten ...			
Negative Außenwirkung	Vertr.	Missbrauch der Daten ...	…führt höchstens zu geringem Ansehensverlust eines Teilbereichs der FU bei einer eingeschränkten Öffentlichkeit	... führt zu einem Ansehensverlust der FU bei einer eingeschränkten Öffentlichkeit oder einem hohen Ansehensverlust eines Teilbereichs der FU	... führt zu einem Ansehensverlust der FU in der breiten Öffentlichkeit
	Integ.	Unberechtigte Manipulation der Daten ...			
	Verfg.	Verlust der Daten ...			
Finanzielle Auswirkungen	Vertr.	Missbrauch der Daten	Summe der finanziellen Auswirkungen < 150.000 €	Summe der finanziellen Auswirkungen < 3.000.000 €	Summe der finanziellen Auswirkungen >= 3.000.000 €
	Integ.	Unberechtigte Manipulation der Daten			
	Verfg.	Verlust der Daten			
daraus resultierender Schutzbedarf:			**normal**	**hoch**	**sehr hoch**

Tabelle 1: 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.

Die praktische Durchführung einer Schutzbedarfsanalyse unter Anwendung der Bewertungstabelle (Tabelle 1, Seite 53) wird im Folgenden kurz skizziert. Es ist keine Beschreibung einer vollständigen Schutzbedarfsanalyse, sondern nur eine fiktive Beispielanalayse.

1. Schritt: Identifikation der zu schützenden Daten

An erster Stelle steht die Identifikation aller Daten, die innerhalb des analysierten Arbeitsprozesses verarbeitet bzw. gespeichert werden. Dies könnten sein:

a. Vorname
b. Nachname
c. Adresse
d. Fachbereichszugehörigkeit
e. Studiengang
f. Prüfungsergebnisse
g. Belegte Seminare

2. Schritt: Ggf. Zusammenfassung der Daten zu Datenkategorien

Häufig können mehrere Einzeldaten inhaltlich zu Datengruppen bzw. -kategorien zusammengefasst werden. Die weiteren Schritte sind dann stets auf die Datenkategorien anzuwenden und nicht mehr auf die dort enthaltenen Einzeldaten. Wenig sinnvoll ist es, Vornamen und den Nachnamen gesondert zu bearbeiten. Darum kann eine Datenkategorie „Name“ gebildet werden. Bei einem konkreten Arbeitsprozess kann die Unterscheidung zwischen Stammdaten und Bewegungsdaten sinnvoll sein.

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

3.1 Gedankenexperiment

Nun ist für jede der sechs Schadenskategorien zu überlegen, welche Folgen die Beeinträchtigung von Vertraulichkeit / Verfügbarkeit / Integrität im schlimmsten Fall hätte.

Zu durchdenken bzgl. der Vertraulichkeit: Vorausgesetzt, Unbefugte erlangen Kenntnis von den Daten, bzw. Datenkategorien welche Folgen hätte dies im schlimmsten Falle auf das informationelle Selbstbestimmungsrecht, auf die persönliche Unversehrtheit und die Aufgabenerfüllung. Es ist nach den finanziellen Auswirkungen und den negativen Auswirkungen auf das Ansehen der Freien Universität Berlin zu fragen und danach, gegen welchen Gesetze, Vorschriften und Verträge hierdurch verstoßen würde.

Zu durchdenken bzgl. der Integrität: Vorausgesetzt, an den Daten wurde unberechtigt manipuliert, welche Folgen …

Zu durchdenken bzgl. der Verfügbarkeit: Vorausgesetzt, die Daten sind verloren, welche Folgen …

Die in den insgesamt 18 Gedankenexperimenten gefundenen möglichen Folgen sollten in einer Tabelle notiert werden.

Beeinträchtigungen (Kategorien)	**Verlust von**	**Bedrohung**	**Auswirkungen**
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Vertr.	Bekannt werden der Daten für Unberechtigte ...	Kollegen werden nicht mehr mit Betroffenem zusammenarbeiten wollen
	Integ.	Unberechtigte Manipulation der Daten ...	Gratifikation erhält ein Unberechtigter
	Verfg.	Verlust der Daten ...	Es kommt nur zu Verzögerungen, ohne inhaltliche Bedeutung
Verstoß gegen andere Gesetze und Vorschriften	Vertr.	Bekannt werden der Daten für Unberechtigte ...	
	Integ.	Unberechtigte Manipulation der Daten ...	Strafbarkeit wegen Urkundenfälschung
	Verfg.	Verlust der Daten ...	
…	Vertr.	…	
	Integ.	…	
	Verfg.	…	

Tabelle 2: Schutzbedarfsbestimmung

3.2 Anwendung der Bewertungsmatrix

Anschließend sind die Ergebnisse zu vergleichen mit den in der Bewertungstabelle vorgegebenen Maßstäben: Sind etwa nur einige Arbeitabläufe beeinträchtigt? Wird die Auftragserfüllung für einen Teilbereich eingeschränkt? Ist der Auftrag der Freien Universität insgesamt gefährdet?

Die jeweils passenden Bewertungen sind eine Tabelle einzutragen. (Muster siehe: Tabelle 3: Beispiel-Ergebnis einer Schutzbedarfsbestimmung)

Beeinträchtigungen (Kategorien)	Verlust von	Bedrohung	Abschätzung des Schadens		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Vertr.	Bekannt werden der Daten für Unberechtigte ...	X		
	Integ.	Unberechtigte Manipulation der Daten ...	X		
	Verfg.	Verlust der Daten ...	X		
Verstoß gegen andere Gesetze und Vorschriften	Vertr.	Bekannt werden der Daten für Unberechtigte ...		X	
	Integ.	Unberechtigte Manipulation der Daten ...	X		
	Verfg.	Verlust der Daten ...		X	
…	Vertr.	…	X		
	Integ.	…	X		
	Verfg.	…	X		
daraus resultierender Schutzbedarf:			**normal**	**hoch**	**sehr hoch**

Tabelle 4: Beispiel-Ergebnis einer Schutzbedarfsbestimmung.

Der höchste Schutzbedarf einer Kategorie bestimmt den Schutzbedarf des IT-Verfahrens. In dem folgenden Beispiel würde das IT-Verfahren in die Schutzklasse „hoch“ eingestuft.

Auf Grund der bisher gemachten Erfahrungen bei der Anwendung der Bewertungstabelle hat sich herausgestellt, dass bei der Bearbeitung der Kategorie „Verstoß gegen Gesetze, Vorschriften und Verträge“ (zweite Zeile in der Tabelle) häufig unklar ist, welche Gesetze und Vorschriften für das betreffende IT-Verfahren besonders relevant sind. Dies sind zunächst einmal die speziellen Regelungen des Verfahrens (z.B. Beamtengesetz, Landeshaushaltsordnung) und daneben allgemeine Vorschriften, die bei jedem IT-Verfahren an der Freien Universität Berlin eine Rolle spielen könnten:

Datenschutzgesetze, beispielsweise

- Berliner Datenschutzgesetz (BlnDSG)
- Informationsverarbeitungsgesetz (IVG)
- Bundesdatenschutzgesetz (BDSG)
- Gesetz zur Förderung der Informationsfreiheit im Land Berlin (Berliner Informationsfreiheitsgesetz – IFG)

Hochschulgesetze bzw. -verordnungen, beispielsweise

- Berliner Hochschulgesetz (BerlHG)
- Studierendendatenverordnung (StudDatVO)
- Landesbeamtengesetz (LBG)

Vorschriften zur Mitbestimmung, beispielsweise

- Landespersonalvertretungsgesetz Berlin (LPersVG-Berlin)

- Tarifvertrag über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informationstechnik
- IT-Rahmendienstvereinbarung der Freien Universität Berlin

Wird der Schutzbedarf in die Schutzklasse „normal“ eingestuft, reichen im Allgemeinen die Maßnahmen des IT-Grundschutzes aus. In allen anderen Fällen, also wenn das IT-Verfahren in die Schutzklasse „hoch“ oder „sehr hoch“ eingestuft wird, muss eine verfahrenspezifische Risikoanalyse durchgeführt werden. (Die Vorgehensweise bei einer Risikoanalyse wird in dem folgenden Kapitel 4 beschrieben.)

Der folgende Ausschnitt aus Abbildung 1 „Modell des IT-Sicherheitsprozesses“ stellt diese unterschiedliche Vorgehensweise in Abhängigkeit des Ergebnisses der Schutzbedarfsanalyse grafisch dar.

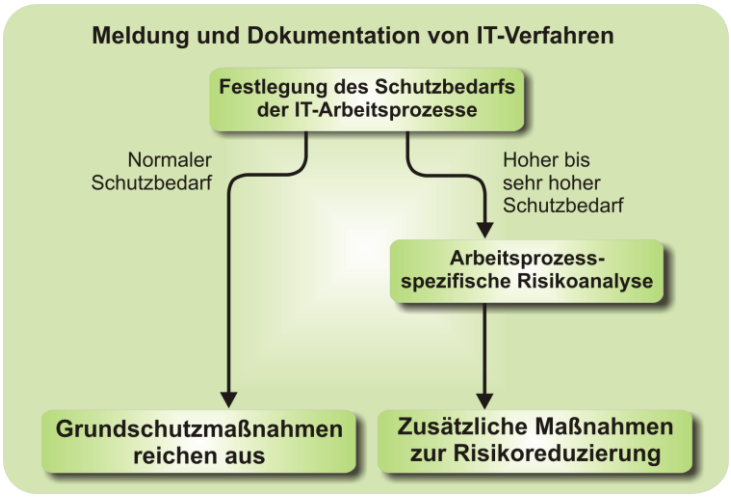
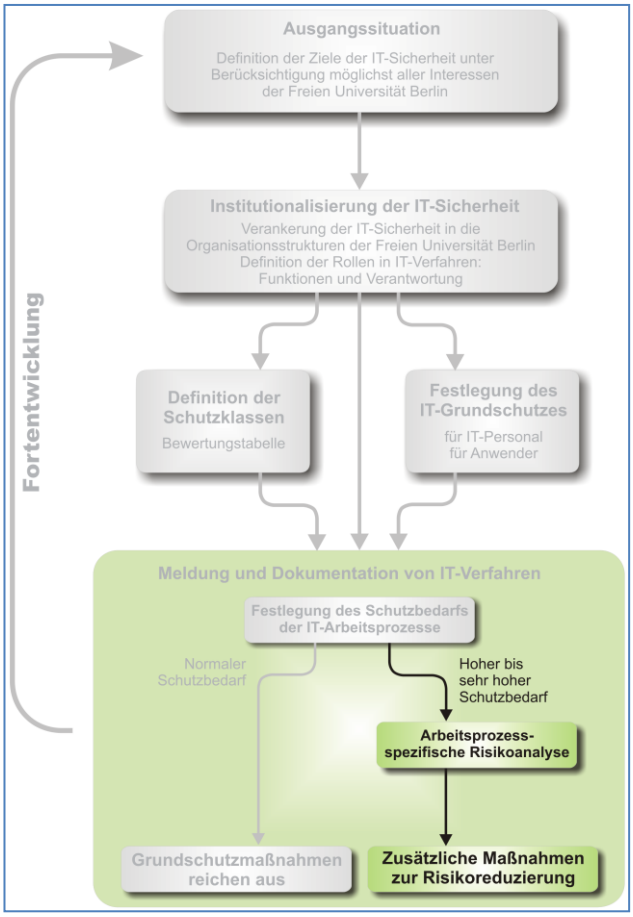


Abbildung 4: Vereinfachte Darstellung der Schutzbedarfsanalyse und der sich daraus ergebenden Konsequenzen.

Die Dokumentation der Schutzbedarfsanalyse besteht aus dem Ergebnis der Bewertungstabelle und weiteren Angaben über den analysierten IT-Arbeitsprozess bzw. das analysierte IT-Verfahren. Zu Beginn ist die Fachaufgabe soweit zu skizzieren, wie es für das Verständnis der Beurteilung des Schutzbedarfs erforderlich ist. Daran anschließend sollten mögliche Schäden in den IT-Verfahren bzw. IT-Arbeitsprozessen dargestellt werden, die bezüglich der drei Grundbedrohungen gegliedert sind. Die Folgen dieser Schäden können dann auf Basis der obigen Bewertungstabelle bewertet werden. Daran kann sich eine kurze Beschreibung des Ist-Zustands der IT-Sicherheitsmaßnahmen anschließen. Gegebenenfalls wird auf wichtige Schwachstellen in den Sicherheitsmaßnahmen kurz hingewiesen. Diese beiden Aspekte sind nicht unmittelbar Gegenstand der Schutzbedarfsanalyse, sie sollten aber in unmittelbarem Zusammenhang mit der Abhandlung der Verfahren erfolgen, um den inhaltlichen Bezug nicht zu verlieren.

4. Risikoanalyse



Für jeden IT-Arbeitsprozess bzw. jedes IT-Verfahren mit hohem oder sehr hohem Schutzbedarf (Schadensstufe „hoch“ und „sehr hoch“) muss eine Bedrohungs- und Risikoanalyse durchgeführt werden. Die dabei ermittelten untragbaren Risiken müssen durch geeignete Maßnahmen auf ein tragbares Maß reduziert werden. Separat für jeden IT-Arbeitsprozess bzw. jedes IT-Verfahren sind die Ergebnisse in geeigneter Weise zu dokumentieren.

Der Begriff „Risiko“ ist definiert als ein Maß für die Gefährdung, die von einer Bedrohung ausgeht. Das Risiko setzt sich zusammen aus zwei Komponenten: die Wahrscheinlichkeit, mit der das Ereignis eintritt, und die Höhe des Schadens, der als Folge des Ereignisses auftritt.

In der Schutzbedarfsanalyse wird – unabhängig von bereits getroffenen Maßnahmen – der mögliche Schadensumfang abgeschätzt („worst case“-Analyse). Die Bewertungstabelle (siehe Tabelle 1, Seite 53) definiert die Schwelle des noch tragbaren Risikos. Ergibt sich ein Schutzbedarf von „hoch“ oder „sehr hoch“, werden in einem zweiten Schritt (Risikoanalyse) – also nach Erkennen der Gefahr – Vorkehrungen und Maßnahmen erarbeitet, um die Wahrscheinlichkeit des Schadenseintritts und damit das Risiko zu reduzieren. Ziel ist es, eine relative Sicherheit herzustellen.

Bei der Bedrohungs- und Risikoanalyse wird vorausgesetzt, dass die im Kapitel IT-Grundschutz vorgesehenen Maßnahmen auch für die hier betrachteten Verfahren umgesetzt werden. Daher werden die dort festgelegten Maßnahmen hier nicht noch einmal aufgeführt. Das Ergebnis der Risikoanalyse beinhaltet somit nur die zusätzlich notwendigen, über den Grundschutz hinausgehenden Maßnahmen.

Zur Durchführung einer Risikoanalyse existieren verschiedene Methoden. Die hier vorgestellte Methode orientiert sich an dem Sicherheitshandbuch des BSI. Zur Durchführung einer Risikoanalyse kann aber auch eine alternative Methode angewendet werden. Die Anwendung einer alternativen Methode sollte in Absprache mit der für die Meldung von IT-Verfahren zuständigen Stelle, zurzeit eAS, erfolgen.

Die Bedrohungs- und Risikoanalyse wird in mehreren Schritten durchgeführt. Zunächst werden alle für den Betrieb eines IT-Verfahrens benötigten Komponenten, Personen usw. (in Anlehnung an die Terminologie des BSI-Grundschutz- und Sicherheitshandbuchs „Objekte“ genannt) erfasst. Anschließend werden systematisch die Risiken bzw. Bedrohungen ermittelt, die an diesen Objekten angreifen können. Die daraus resultierenden Schäden werden nach der im Kapitel 3 Schutzbedarfsanalyse verwendeten dreiteiligen Werteskala (siehe Tabelle 1, Seite 53) klassifiziert. Danach wird eine Abschätzung vorgenommen, bei der ermittelt werden soll, mit welcher Wahrscheinlichkeit ein Schaden in dieser Höhe zu erwarten ist. Hierfür wird wiederum eine Skala mit Werten von „häufig“ bis „praktisch nie“ verwendet, wobei den Werten die in der folgenden Tabelle aufgeführten Bedeutungen unterlegt werden.

Bedeutung	Beschreibung
praktisch nie	Das Schadensereignis tritt praktisch nie auf und wird daher nicht betrachtet. (z.B. Erdbeben)
sehr selten	Das Eintreten des Schadensereignis ist nicht auszuschließen, tritt aber nur sehr selten auf (alle 50 bis 100 Jahre, z.B. Brand)
selten	Das Schadensereignis tritt alle paar Jahre einmal auf (z.B. Festplattenausfall)
öfter	Das Schadensereignis tritt alle paar Monate einmal auf (z.B. Bandfehler bei Backup/Restore, versehentliches Löschen von Daten)
häufig	Das Schadensereignis tritt alle paar Wochen einmal auf (z.B. Ausfall der Netzwerkverbindung; Eingabefehler)

Tabelle 5: Häufigkeitswerte der Eintrittswahrscheinlichkeit von Schäden.

Das Risiko, das aus einer Bedrohung erwächst, wird bestimmt durch die Höhe des Schadens und die relative Häufigkeit des Eintretens der Bedrohung. Mathematisch ausgedrückt ist das Risiko der Erwartungswert für den Schaden pro Zeiteinheit. Das Risiko wird also beschrieben durch das Wertepaar Schadenshöhe und Schadenshäufigkeit. Es wird unterschieden zwischen tragbaren und untragbaren Risiken.

Die Zuordnung von Risiken zu einer bestimmten Kategorie erfolgt anhand der nachstehenden Tabelle 6. Dabei bedeuten

Untragbar – untragbares Risiko,

Tragbar – noch tragbares Risiko.

Untragbare Risiken müssen durch zusätzliche Maßnahmen auf das für die Freie Universität tragbare Maß reduziert werden. Der Verfahrensverantwortliche hat zu entscheiden, ob durch die verwirklichten Schutzmaßnahmen das Risiko tragbar und somit der Betrieb des IT-Verfahren in der vorgesehenen Form verantwortbar für die Freie Universität Berlin ist.

Schadenswert / Häufigkeit	**normal** 1	**hoch** 2	**sehr hoch** 3
praktisch nie	Tragbar	Tragbar	Tragbar
sehr selten	Tragbar	Tragbar	Untragbar
selten	Tragbar	Untragbar	Untragbar
öfter	Untragbar	Untragbar	Untragbar
häufig	Untragbar	Untragbar	Untragbar

Tabelle 6: Risikoklassen

Zusammenfassend sind folgende Schritte für die Risikoanalyse durchzuführen:

Schritt 1: Erfassung der für den IT-Arbeitsprozess bzw. das IT-Verfahren relevanten und bedrohten Objekte
Hilfsmittel: Sicherheitshandbuch des BSI [Sicherheitshandbuch, Anhang 3]

Schritt 2: Bewertung des Schutzbedarfs der Objekte
Hilfsmittel: Bewertungsmatrix (Seite 53)

Schritt 3: Bestimmung der Häufigkeit von Schäden
Hilfsmittel: Tabelle der Häufigkeitswerte (Seite 59)

Schritt 4: Zusammenstellung und Bewertung (Klassifizierung) der Risiken
Hilfsmittel: Tabelle der Risikoklassen (Seite 60)

Schritt 5: Maßnahmen zur Reduzierung der untragbaren Risiken
Hilfsmittel: Sicherheitshandbuch des BSI [Sicherheitshandbuch, Kapitel 6.2]

Das Ergebnis der Bedrohungs- und Risikoanalyse (Schritt 4) wird dann in einer einzigen Tabelle (Ergebnistabelle) zusammengefasst. Darüber hinaus wird der Bezug zu den Grundbedrohungen Verlust der Verfügbarkeit (Verfügb.), Integrität (Integrit.) und Vertraulichkeit (Vertraul.) hergestellt. In der letzten Spalte werden stichwortartig die Maßnahmen genannt, die zur Risikoreduzierung eingesetzt werden sollen (Schritt 5). Eine ausführliche Erläuterung der Maßnahmen erfolgt im Anschluss an die Tabelle unter dem jeweiligen Stichwort. Ziel der Umsetzung der genannten Maßnahmen ist die Reduzierung der Risiken auf ein tragbares Maß.

Anhand eines fiktiven Beispiels soll gezeigt werden, wie eine Ergebnistabelle aussehen könnte. Diese umfasst nur eine Auswahl von möglichen Bedrohungen nebst Bewertungen und Maßnahmen. Naturgemäß ist diese Auswahl unvollständig. Wie aus dem Beispiel ersichtlich, können auch bei tragbaren Risiken zusätzliche Maßnahmen ergriffen werden, wenn damit die Grundsätze der Wirtschaftlichkeit nicht verletzt werden.

Im konkreten Fall müssen verfahrenspezifische Bedrohungen und Bewertungen, sowie ggf. geeignete Maßnahmen zur Risikoreduzierung ausgearbeitet werden.

(Hinweis: Die Beispieltabelle erstreckt sich über die folgenden drei Seiten. Es handelt sich um ein fiktives Beispiel, dem keine reale Risikoanalyse zugrunde liegt.)

Bezeichnung der Bedrohung	Grund-bedroh-ung	Bedrohtes Objekt bzw. Objektgruppe	Schadenswert	Häufigkeit	Risikoklasse	Maßnahmen
– Hardware –						
Technisches Versagen	Verfügb.	Produktivsystem, PDC	3	sehr selten	Un-trag-bar	M-01: Wartungsvertrag Produktivsystem und PDC
	Verfügb.	Weitere Server	2	sehr selten	Trag-bar	M-02: Wartungsvertrag weitere Server
	Verfügb.	Arbeitsplatz-PCs	1	selten	Trag-bar	
	Verfügb.	Drucker	1	selten	Trag-bar	
	Verfügb.	Zentrale Netzwerkkom-ponenten	1	selten	Trag-bar	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Diebstahl	Verfügb. Vertraul.	Server	2	selten	Un-trag-bar	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude M-14: Zugriffsschutz Server
Spannungsschwan-kungen, Blitzschlag	Verfügb.	Produktivsystem, PDC	2	sehr selten	Trag-bar	M-07: Unterbrechungsfreie Stromversorgung
	Verfügb.	Weitere Server	1	sehr selten	Trag-bar	M-07: Unterbrechungsfreie Stromversorgung
Fehlbedienung	Vertraul. Integrit.		1	sehr selten	Trag-bar	
Sabotage	Verfügb.	Produktivsystem, PDC	1	sehr selten	Trag-bar	
	Verfügb.	Weitere Server	1	sehr selten	Trag-bar	
Unkontrollierter Zu-gang	Verfügb. Integrit. Vertraul.	Zentrale Server	2	selten	Un-trag-bar	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude M-14: Zugriffsschutz Server
	Integrit. Vertraul.	Clients	1	selten	Trag-bar	M-08: Zugangsschutz Clients
– Infrastruktur –						
Höhere Gewalt, Ter-ror, Vandalismus	Verfügb.	Serverraum	1	prak-tisch nie	Trag-bar	
	Verfügb.	Zentrale Netzkompo-nenten	1	sehr selten	Trag-bar	
Feuer	Verfügb.	Serverraum	1	sehr selten	Trag-bar	
	Verfügb.	Netzkomponenten	1	sehr selten	Trag-bar	
Wasser	Verfügb.	Serverraum	1	sehr selten	Trag-bar	
	Verfügb.	Netzkomponenten	1	sehr selten	Trag-bar	
Überhitzung	Verfügb.	Serverraum	1	öfter	Un-trag-bar	M-09: Klimatisierung

Bezeichnung der Bedrohung	Grund-bedroh-ung	Bedrohtes Objekt bzw. Objektgruppe	Schadenswert	Häufigkeit	Risikoklasse	Maßnahmen
Ausfall der Stromver-sorgung	Verfügb.	Zentrale Hardware	1	sehr selten	Trag-bar	M-07: Unterbrechungsfreie Stromversorgung
Unbefugter Zugang	Vertraul.	Serverraum	2	sehr selten	Trag-bar	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude
	Vertraul.	Arbeitsräume	1	selten	Trag-bar	M-10: Nicht öffentliche Räume
– Kommunikation –						
Ausfall	Verfügb.	Netzwerk	2	sehr selten	Trag-bar	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Überlastung	Verfügb.	Netzwerk	1	selten	Trag-bar	
Abhören	Vertraul.	Netzwerk	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung
Manipulation	Vertraul. Integrit.	Netzwerk	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung
Anschließen zusätzli-cher Endgeräte	Vertraul. Integrit.	Personenbezogene Daten	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Zugangsschutz Netzkomponenten
Unerlaubter Zugang	Vertraul. Integrit.	Netzwerk	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung
– Datenträger –						
Unkontrollierter Zu-griff	Verfügb. Integrit. Vertraul.	Sicherungsbänder	2	sehr selten	Trag-bar	M-12: Verschlüsselung der Datensicherung, Zu-gangsschutz
Beschädigung	Verfügb. Integrit.	Sicherungsbänder	1	sehr selten	Trag-bar	
	Verfügb. Integrit.	Festplatten	1	sehr selten	Trag-bar	M-13: RAID-5-System, Spiegelplatten
Fehlerhafte Erzeu-gung	Verfügb. Integrit.	Datenträger	1	sehr selten	Trag-bar	
Unzureichende Ent-sorgung	Vertraul.	Datenträger	2	prak-tisch nie	Trag-bar	
Diebstahl	Verfügb. Vertraul.	Datenträger	2	sehr selten	Trag-bar	M-12: Verschlüsselung der Datensicherung, Zu-gangsschutz
– Software, Daten –						
Unerlaubtes Aufspie-len von Software	Verfügb.	Software, Daten	1	sehr selten	Trag-bar	M-14: Zugriffsschutz Server
Fehlbedienung	Verfügb. Integrit. Vertraul.	Betriebssystem, Daten-bank	1	sehr selten	Trag-bar	
Unerlaubter Zugriff und Einblick	Integrit. Vertraul.	Datenbank, Daten, Passwörter	2	sehr selten	Trag-bar	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude M-14: Zugriffsschutz Server
Mangelhafte Verwal-tung der Zugriffsrech-te	Integrit. Vertraul.	Datenbank	2	selten	Un-trag-bar	M-15: Rollentrennung
Schadprogramme (Computerviren)	Verfügb. Integrit.	Betriebssystem	1	sehr selten	Trag-bar	

Bezeichnung der Bedrohung	Grund-bedroh-ung	Bedrohtes Objekt bzw. Objektgruppe	Schadenswert	Häufigkeit	Risikoklasse	Maßnahmen
	Vertraul. Integrit.	Clients	1	öfter	Un-trag-bar	M-16: Virenscanner
– Papier –						
Unvollständigkeit, mangelnde Aktualität	Verfügb.	Systemdokumentation	1	sehr selten	Trag-bar	
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Trag-bar	
Unzureichende Ent-sorgung	Vertraul.	Systemdokumentation	1	sehr selten	Trag-bar	
	Vertraul.	Personenbezogene Daten	2	selten	Un-trag-bar	M-17: Schredder
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Trag-bar	
– Personen –						
Ausfall	Verfügb.	Administratoren, Appli-kationsbetreuer	2	sehr selten	Trag-bar	M-18: Vertretung
Unkenntnis	Verfügb. Integrit. Vertraul.	Administratoren, Appli-kationsbetreuer	1	sehr selten	Trag-bar	
	Integrit. Vertraul.	Anwender	1	sehr selten	Trag-bar	
Überlastung	Verfügb. Integrit. Vertraul.	Administratoren, Appli-kationsbetreuer	2	sehr selten	Trag-bar	M-15: Rollentrennung M-18: Vertretung
	Integrit. Vertraul.	Anwender	1	sehr selten	Trag-bar	
Fehlende Kontrollen und Regelungen	Verfügb. Integrit. Vertraul.	Administratoren, Appli-kationsbetreuer	2	sehr selten	Trag-bar	M-19: Kontrolle der Akteure
	Integrit. Vertraul.	Anwender	2	sehr selten	Trag-bar	M-19: Kontrolle der Akteure
Nachlässige Pass-worthandhabung	Vertraul.	Passwörter	2	sehr selten	Trag-bar	M-20: Festlegung der Passwortregeln
Kriminelle Absicht	Verfügb. Integrit. Vertraul.	Administratoren, Appli-kationsbetreuer, An-wender	2	sehr selten	Trag-bar	M-15: Rollentrennung M-21: Kontrolle der Proto-koll-Dateien
	Verfügb. Integrit. Vertraul.	Externe	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung M-06: Zugangsschutz M-14: Zugriffsschutz

Tabelle 7: Fiktive Beispieltabelle für eine Bedrohungs- und Risikoanalyse.

Die in der Tabelle rechts aufgeführten Maßnahmen müssen im Anschluss unter dem jeweiligen Stichwort (z.B.: „M-14: Zugriffsschutz“) einzeln erläutert werden. Beispielhaft werden nachfolgend drei Maßnahmen wiedergegeben. Ebenso wie bei der obigen Tabelle handelt es sich um fiktive Beispiele.

M-01: Wartungsvertrag Produktivsystem und PDC

Zur Gewährleistung der Verfügbarkeit des Produktivsystems wurde ein Servicevertrag mit dem Hersteller der Hardware, Firma XYZ, abgeschlossen. Dieser Vertrag sieht vor, dass innerhalb von 6 Stunden ein Fehler (Fixzeit) behoben werden muss. Die Unterlagen zu den genannten Verträgen sind im Fachbereich XY, in der Fachbereichsverwaltung abgelegt.

M-02: Wartungsvertrag weitere Server

Ein weiterer Service-Vertrag mit dem Hardwareproduzenten soll die Verfügbarkeit der übrigen Server gewährleisten. In diesem Vertrag wurden alle Server einbezogen, die zur Aufrechterhaltung des Betriebs notwendig sind. Insbesondere handelt es sich dabei um die Server der Domänenverwaltung (Primärer Domänencontroller und Backup Domänencontroller) und den Printserver. Der Vertrag dieser Rechnersysteme sieht eine 4-stündige Reaktionszeit und eine „Next Day Fixzeit“ vor, d.h. bis zum jeweils nächsten Werktag muss ein Fehler behoben werden. Die Unterlagen zu den genannten Verträgen sind im Fachbereich XY, in der Fachbereichsverwaltung abgelegt.

(…)

M-06: Zugangsschutz Serverraum, gesichertes Gebäude

Der Serverraum in dem Gebäude XY, Beispielstraße 99 ist vor unbefugtem Zutritt geschützt. Der Raum besitzt eine Tür, die stets verschlossen gehalten wird. Die Tür besitzt keine Außenklinke und kann von außen nur über einen Transponder (mit gültiger Codierung) geöffnet werden. Von innen kann die Tür über eine Klinke geöffnet werden.

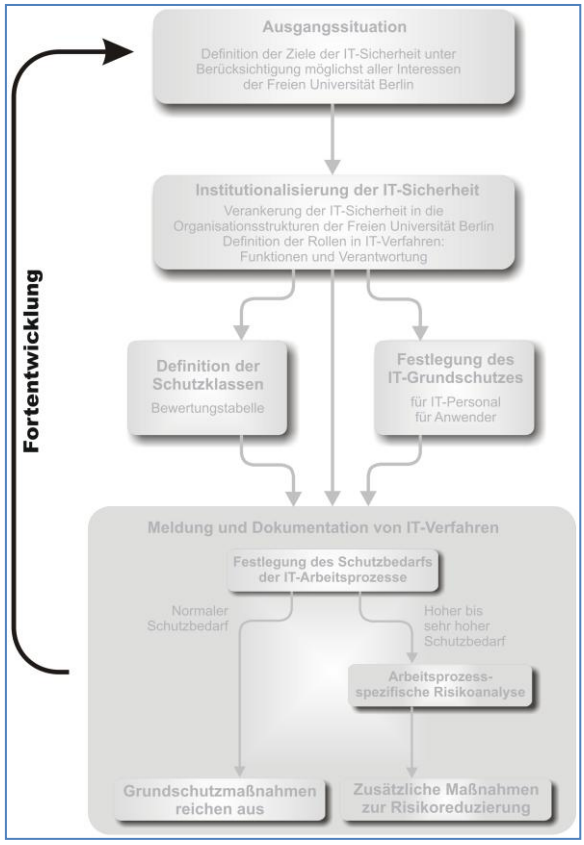
Außerdem verfügt der Serverraum über zwei Fenster. Beide Fenster sind stets verschlossen und mit einer massiven Stahljalousie von außen geschützt. Diese Jalousie wird durch Stahlbolzen verankert und ist zur Einbruchsprävention geeignet.

Alle Fenster und Türen des gesamten Gebäudes werden durch Stahljalousien geschützt. Bei der Eingangstür handelt es sich um eine massive Eisentür, die durch zwei Schlösser gesichert ist. Alle Stahljalousien werden bei Betätigung eines zentralen Schlüsselschalters neben der Eingangstür herabgelassen. Die Stahljalousie der Eingangstür kann mit dem gleichen Schlüsselschalter geöffnet werden. Die übrigen Jalousien bleiben unten; sie müssen separat über Schalter in den Räumen einzeln hochgezogen werden.

(…)

5. Umsetzung der IT-Sicherheitsrichtlinie

Aufgrund der hohen Eigenständigkeit der einzelnen Organisationseinheiten ist eine zentrale Kontrolle der Umsetzung nicht vorgesehen, vielmehr wird – in Übereinstimmung mit Abschnitt 1.3 „Verantwortlichkeiten und Organisation der IT-Sicherheit“ – die Verantwortung für die Umsetzung auf die einzelnen Organisationseinheiten verteilt. Die entscheidenden Impulse sollen dabei von den IT-Verantwortlichen ausgehen.



Die Verbreitung und Umsetzung der IT-Sicherheitsrichtlinie soll nach folgendem, gemeinsam mit den IT-Verantwortlichen der Organisationseinheiten abgesprochenen Vorgehen geschehen.

5.1. Inkraftsetzen der IT-Sicherheitsrichtlinie

- Die IT-Sicherheitsrichtlinie wurde als FU-Rundschreiben V11/05 am 10. August 2005 universitätsweit veröffentlicht.
- Nach jeder regelmäßig stattgefundenen Aktualisierung (Fortschreibung) der Richtlinie wird diese in Form eines FU-Rundschreibens an die Organisationseinheiten der Freien Universität Berlin verteilt und ist damit verbindlich.

Verantwortlich für Initiierung: AG IT-Sicherheit Verantwortlich für Umsetzung: Präsidium	Termin: Nach jeder Aktualisierung der IT-Sicherheitsrichtlinie

5.2. Information der Mitarbeiter

- Innerhalb der Organisationseinheiten ist sicherzustellen, dass alle Mitarbeiter die für sie relevanten Teile der IT-Sicherheitsrichtlinie kennen und beachten. Insbesondere ist zu gewährleisten, dass zukünftig
  - für das leitende Personal die allgemeinen Grundsätze und die Organisation der Sicherheit,
  - für alle Anwender die Maßnahmen des IT-Grundschutzes für IT-Anwender,

- für alle Beschäftigten im IT-Bereich die Maßnahmen des IT-Grundschutzes für IT-Personal,
- für alle Verfahrensverantwortlichen die verfahrenspezifischen Regelungen

als bekannt voraus gesetzt werden können.

Verantwortlich: Bereichsleiter	Termin: nach jeder Aktualisierung der IT-Sicherheitsrichtlinie

Neue Mitarbeiter müssen auf die geltende IT-Sicherheitsrichtlinie bei der Einstellung hingewiesen werden. Bei Aufnahme ihrer Tätigkeit müssen sie über die für sie maßgeblichen Bestimmungen der IT-Sicherheitsrichtlinie informiert werden.

Verantwortlich bei Einstellung: Personalstelle Verantwortlich bei Tätigkeitsaufnahme: Bereichsleiter	Termin: bei Dienstantritt

5.3. Umsetzung des IT-Grundschutzes

Die Gesamtverantwortung für die Umsetzung der verfahrensspezifischen Maßnahmen des IT-Grundschutzes liegt bei den IT-Verantwortlichen der Organisationseinheiten. Bei der Anwendung einzelner Grundschutzmaßnahmen sind die bei jeder Maßnahme angegebenen Verantwortlichkeiten über die Initiierung und Umsetzung zu beachten.

Ist eine einvernehmliche Lösung bei Differenzen über die Umsetzung der Maßnahmen in einem Bereich nicht möglich, kann das CIO-Gremium über die internen Vorgänge informiert werden. Das CIO-Gremium trifft auf Basis der geltenden Richtlinien eine Entscheidung in der strittigen Sache.

Stellt eine Stelle in der Freien Universität Berlin einen Mangel in einem IT-Verfahren fest, der zu gravierenden Schäden führen kann, ist der IT-Sicherheitsbeauftragte über den Tatbestand zu informieren. Der IT-Sicherheitsbeauftragte versucht kurzfristig in Einvernehmen mit allen Beteiligten eine Lösung für das Sicherheitsproblem zu finden. Falls eine Lösung im Einvernehmen nicht hergestellt werden kann, informiert der IT-Sicherheitsbeauftragte das CIO-Gremium. Das CIO-Gremium entscheidet über das weitere Vorgehen.

5.4. Fortschreibungs- und Berichtspflicht

Die IT-Sicherheitsrichtlinie bedarf der ständigen Überarbeitung und Weiterentwicklung. Veränderungen in der Bedrohungssituation oder technische Entwicklungen sind zu berücksichtigen. Turnusmäßig (z.B. im Zusammenhang mit der Fortschreibung der IT-Sicherheitsrichtlinie) werden die Aufzeichnungen zu aufgetretenen Sicherheitsproblemen ausgewertet. Bei Bedarf werden zusätzliche Maßnahmen in den

Grundschutzkatalog aufgenommen und ggf. auch Maßnahmen wieder aufgehoben bzw. ersetzt, die sich nicht bewährt haben.

Mit der vorliegenden IT-Sicherheitsrichtlinie werden Grundlagen und Werkzeuge bereitgestellt, mit deren Hilfe die angestrebte Sicherheit gewährleistet und so schrittweise ein ausreichendes Sicherheitsniveau erreicht werden kann. Dies ist ein kontinuierlicher Prozess, der die konstruktive Zusammenarbeit aller Beteiligten erfordert.

6. Glossar

Administrator
Konfiguriert und betreibt →IT-Systeme

AG IT-Sicherheit
Die Arbeitsgruppe IT-Sicherheit setzt sich aus Vertretern verschiedener Organisationseinheiten der Freien Universität und der Datenschutzbeauftragten unter dem Vorsitz des →IT-Sicherheitsbeauftragten zusammen. Zu den wesentlichen Aufgaben der Arbeitsgruppe gehören u. a. die Entwicklung von IT-Sicherheitszielen und -strategien sowie der →IT-Sicherheitsrichtlinie. Darüber hinaus initiiert, steuert und kontrolliert sie den IT-Sicherheitsprozess.

Anwender
Endbenutzer von →IT-Systemen

Anwenderbetreuung / Hotline
Installiert und wartet Endgeräte und ist die erste Hilfe für den Anwender bei Problemen im Umgang mit Informationstechnik. Kann das Problem nicht sofort gelöst werden, wird eine weitere Hilfestellung organisiert (z.B. →Key-User, →Anwendungsbetreuer).

Anwendungsbetreuung
Passt Anwendungen innerhalb eines →IT-Verfahrens an die Anforderungen der Organisation an. Dies geschieht in enger Zusammenarbeit mit dem Verfahrensverantwortlichen, den Systemadministratoren und den →Key-Usern.

Arbeitsplatzrechner (APC)
Endgerät für die Aufgaben des →Anwenders

Auftragsdatenverarbeitung
Verarbeitung von Daten im Auftrag durch andere Stellen. Für die Verarbeitung personenbezogener Daten im Auftrag gilt §3 BlnDSG.

Authentisierung
Nachweis, dass ein Nutzer das Zielsystem benutzen darf. Authentisierung erfolgt z.B. durch Passwörter. Authentisierung darf nicht mit Identifizierung verwechselt werden: Bei der Identifizierung wird festgestellt, dass eine bestimmte Person mit einer bestimmte Identität übereinstimmt. Authentisierung hingegen stellt nur fest, dass ein Benutzer Kenntnisse (z.B. bei Verwendung eines →Passwortes) oder Dinge (z.B. bei Verwendung von Smartcards) hat, die ihn zur Benutzung eines Systems berechtigen.

Backbone
Gesonderte Netzwerk-Infrastruktur zur Verbindung einzelner eigenständiger Netzwerke mit hoher Geschwindigkeit und meist eigener Administration. Backbone-Kabel verbinden mehrere eigenständige →LAN-Netzsegmente zu einem größeren Netzwerkverbund

Berliner Datenschutzgesetz (BlnDSG)
Regelungen des Landes Berlin zum Schutz personenbezogener Daten, vgl. auch Bundesdatenschutzgesetz (BDSG)

Betriebssystem
Die Aufgabe des Betriebsystems ist das geordnete Zusammenwirken und Steuern aller Geräte und Programme eines Computersystems.

BSI
Bundesamt für Sicherheit in der Informationstechnik des Bundesinnenministeriums (www.bsi.de)

Datenschutz
Regelungen und Maßnahmen für die Verarbeitung personenbezogener Daten

Datensicherheit
Sicherstellung von →Integrität, →Vertraulichkeit und →Verfügbarkeit von Daten

Datensicherung
Kopieren der Daten auf einen zusätzlichen →Datenträger. So ist bei Verlust des Originales noch eine Verfügbarkeit der Daten gewährleistet.

Datenträger
Medium zum Speichern der Daten wie Magnetbänder, Festplatte, CD-ROM, DVD oder USB-Stick

E-Mail
Elektronische Post zum Versenden und Empfangen von Texten und Dateien. Der Transport erfolgt standardmäßig unverschlüsselt (analog zur Postkarte).

Firewall
Netzkomponente, die den Datenverkehr aus/in Netzsegmente/n unter definierten Sicherheitsaspekten regelt

Grundschutz für Anwender
Schreibt allen →Anwendern der Freien Universität Berlin einen einheitlichen Katalog von Sicherheitsmaßnahmen im Umgang mit Informationstechnik vor, um einen definierten Grundschutz zu erlangen.

Integrität
Die Integrität eines Dokumentes versichert dessen Vollständigkeit und Unversehrtheit, d.h. für den Empfänger, dass das Dokument in der geprüften Form auch so vom Absender erstellt wurde.

IT
Informationstechnik

IT-Arbeitsprozess

Ein IT-Arbeitsprozess ist eine sequenzielle und/oder parallele Abfolge von zusammenhängenden IT-gestützten und/oder IT-unterstützenden Tätigkeiten. Ein oder mehrere IT-Arbeitsprozesse bilden ein →IT-Verfahren.

IT-Grundschutzhandbuch

Im IT-Grundschutzhandbuch werden Standardsicherheitsmaßnahmen für typische →IT-Systeme empfohlen, herausgegeben vom →BSI (http://www.bsi.de/gshb/deutsch/menue.htm)

IT-Grundschutz für IT-Personal

Hierin werden allen IT-Mitarbeitern ergänzende Handlungsanweisungen zur Umsetzung des Grundschutzes für →Anwender an die Hand gegeben.

IT-Personal

Sind System- und Netzadministratoren, PC-Servicemitarbeiter, Verfahrensbetreuer, Programmentwickler, IT-Verfahrensverantwortliche und IT-Bereichsverantwortliche

IT-Sicherheitsbeauftragter

ist zuständig für alle IT-Sicherheitsfragen, die Erstellung einer →IT-Sicherheitsrichtlinie, wirkt mit im IT-Sicherheitsprozess und führt den Vorsitz in der →AG IT-Sicherheit. Außerdem koordiniert er die Erstellung von weiteren Konzepten zur IT-Sicherheit.

IT-Sicherheitsrichtlinie

ist eine systematische Bestandsaufnahme und Analyse der Anforderungen und Maßnahmenplanung für den Bereich der IT-Sicherheit der Freien Universität. Es beschreibt die Ziele und Organisation von IT-Sicherheit sowie deren praktische Umsetzung, um die →Verfügbarkeit, →Vertraulichkeit und →Integrität der Verarbeitung von Daten in den →IT-Verfahren zu gewährleisten. (Üblicherweise ist die Bezeichnung „IT-Sicherheitskonzept“ gebräuchlich. Der Begriff „Richtlinie“ wurde gewählt, um die Verbindlichkeit der Regelungen und Maßnahmen zu unterstreichen.)

IT-Systeme

Oberbegriff für Geräte und Programme zur Datenverarbeitung

IT-Verfahren

Ein IT-Verfahren ist eine Zusammenfassung IT-gestützter Arbeitsabläufe. Sie werden beschrieben unter Angabe der technischen und organisatorischen Konzepte und Maßnahmen. Beispiele für IT-Verfahren: SAP R/3 HR in der Personalverwaltung, ALEPH 500 in den Bibliotheken der Freien Universität.

Key-User

besonders geschulte →Anwender, die erste Ansprechpartner bei aufgabenbezogenen Problemen des IT-Einsatzes sind. Sie geben ihre besonderen Kenntnisse an die Anwender weiter (Multiplikatoren).

LAN
Local Area Network – ist das im Haus/Campus verlegte Datennetz

Mengengerüst
Angaben über die Mengen aller in dem betreffenden Zusammenhang interessierenden Ressourcen

Netzknoten
Netzwerkkomponenten, die für den Weitertransport von Daten zwischen Rechnersystemen und →Netzwerksegmenten verantwortlich sind

Netzwerksegmente
Logisch oder physisch getrennte Teile eines Netzwerkes

Passwort
Geheimer Schlüssel, um den unbefugten Zugang zu einem persönlichen Datenbereich zu verhindern

Risiko
Risiko ist ein Maß für die Gefährdung, die von einer Bedrohung ausgeht. Es setzt sich zusammen aus zwei Komponenten: der Wahrscheinlichkeit, mit der das Ereignis eintritt, und der Höhe des Schadens, der als Folge des Ereignisses auftritt.

Rolle
Eine Rolle bündelt die Kompetenzen, die zur Bearbeitung von Aufgaben innerhalb eines IT-gestützten Geschäftsprozesses benötigt werden. Sie beschreibt somit, für welche Aufgaben man mit welchen Rechten auf welche Ressourcen zugreift.

Schützenswerte Daten
Sind Daten, deren Verlust, Bekanntwerden oder Verfälschung einen erheblichen materiellen und immateriellen Schaden bedeutet (siehe Kapitel 3 Schutzbedarfsanalyse)

Server
Zentrale Systeme, auf denen Daten und Programme für eine Gruppe von Anwendern zur Verfügung gestellt werden

Verfügbarkeit
Wahrscheinlichkeit, ein System oder einen Dienst zu einem vorgegebenen Zeitpunkt in einem funktionsfähigen Zustand anzutreffen

Verschlüsselung
Schützt Daten vor der Einsicht durch Dritte. Nur berechtigte Personen können die Daten wieder entschlüsseln und verwenden.

Vertraulichkeit
Die Wahrung der Privatsphäre und der Schutz der personenbezogenen Daten

Viren

Schadprogramme, meist unsichtbar über →E-Mail-Anhänge oder →Datenträger auf den Arbeitsplatzrechner geladen, die bei Ausführung leichten bis schweren Schaden hervorrufen können

Virenscanner

Entsprechende Programme, die in der Lage sind, Schadprogramme zu identifizieren. Wegen der schnellen Entwicklung und Verbreitung neuer Viren ist der Virenscanner immer auf dem neuesten Stand zu halten.

Zugriffsrecht

Wird vom →Administrator vergeben und bezeichnet die Möglichkeiten, bestimmte Daten und Verfahren zu verwenden und zu bearbeiten (z.B. lesen, ausführen, ändern, löschen)

Zuständige Stelle

Dieser Begriff wird in der IT-Sicherheitsrichtlinie immer dann verwendet, wenn die betreffenden Personen oder Dienststellen, die bestimmte Aufgaben wahrnehmen bzw. für bestimmte Sachverhalte zuständig sind, je nach Organisationseinheit innerhalb der Freien Universität unterschiedlich sein können.

ZUV

Zentrale Universitätsverwaltung

7. Literaturverzeichnis

[Sicherheitshandbuch]
Handbuch für die sichere Anwendung der Informationstechnik (IT)
IT-Sicherheitshandbuch, Version 1.0, März 1992, BSI 7105,
Quelle: http://www.bsi.bund.de/literat/kriterie.htm

[Grundschutz-Kataloge]
IT-Grundschutz-Kataloge,
2006, Schriftenreihe zur IT-Sicherheit, BSI,
Quelle: http://www.bsi.bund.de/gshb/deutsch/index.htm

[BSI-Standards zur IT-Sicherheit]
IT-Sicherheitsmanagement und IT-Grundschutz,
Version 1.0, 2005, BSI,
Quelle: http://www.bsi.bund.de/literat/bsi_standard/index.htm

[Daten-Kommunikationsverbindungen]
Konzept für sichere Daten-Kommunikationsverbindungen
November 2002
Quelle: ZEDAT, AG Netze

[Grundschutzheft]
Informationen zum IT-Grundschutz
Freie Universität Berlin, Juni 2006