

# **IT-Sicherheitsrahmenrichtlinie für die Freie Universität Berlin**

Fassung: Mai 2005  
Version 1.9

# Gliederung

## 1. IT-Sicherheit im Bereich der Freien Universität Berlin

- Ausgangssituation
- Erläuterungen zu den wichtigsten Grundbegriffen
- Verantwortlichkeiten und Organisation der IT-Sicherheit

## 2. Definition des Grundschutzes

- Regeln des IT-Grundschutzes für IT-Anwender
- Regeln des IT-Grundschutzes für IT-Personal

## 3. Schutzbedarfsanalyse

- Bewertungsmaßstab

## 4. Risikoanalyse

- Detaillierte Bedrohungs- und Risikoanalyse für jene IT-Verfahren, die in einer Schadensstufe > 2 (mittlerer Schaden) eingeordnet wurden.

## 5. Umsetzung der IT-Sicherheitsrahmenrichtlinie

- Maßnahmen zur Umsetzung der IT-Sicherheitsrahmenrichtlinie

## 6. Anhang

- Technische Infrastruktur (Beschreibung der Netzinfrastruktur)

# Inhaltsverzeichnis

<b>Gliederung.....</b>	<b>1</b>
<b>Inhaltsverzeichnis .....</b>	<b>2</b>
<b>Versionsstand und Dokumentenstatus .....</b>	<b>4</b>
<b>Vorbemerkung .....</b>	<b>5</b>
<b>1. Ausgangssituation .....</b>	<b>7</b>
1.1. Grundbegriffe der IT-Sicherheitsrahmenrichtlinie .....	9
1.2. IT-Verfahren .....	10
1.3. Verantwortlichkeiten und Organisation der IT-Sicherheit .....	13
<b>2. Definition des Grundschatzes.....</b>	<b>14</b>
2.1. Maßnahmen des IT-Grundschatzes für IT-Anwender .....	16
2.1.1. Allgemeines .....	16
2.1.2. Sicherung der Infrastruktur .....	16
2.1.3. Hard- und Software .....	17
2.1.4. Zugriffsschutz .....	18
2.1.5. Kommunikationssicherheit.....	20
2.1.6. Datensicherung .....	20
2.1.7. Umgang mit Datenträgern .....	21
2.1.8. Schützenswerte Daten .....	22
2.2. Maßnahmen des IT-Grundschatzes für IT-Personal .....	22
2.2.1. Allgemeines .....	23
2.2.2. Organisation von IT-Sicherheit .....	23
2.2.3. Personelle Maßnahmen .....	27
2.2.4. Sicherung der Infrastruktur .....	28
2.2.5. Hard- und Softwareeinsatz .....	32
2.2.6. Zugriffsschutz .....	35
2.2.7. System- und Netzwerkmanagement.....	39
2.2.8. Kommunikationssicherheit.....	40
2.2.9. Datensicherung .....	42
2.2.10. Datenträgerkontrolle .....	43
<b>3. Schutzbedarfsanalyse.....</b>	<b>46</b>
<b>4. Risikoanalyse .....</b>	<b>50</b>
<b>5. Umsetzung der IT-Sicherheitsrahmenrichtlinie .....</b>	<b>57</b>
5.1. Publikation der IT-Sicherheitsrahmenrichtlinie, insbesondere der IT- Grundschatzmaßnahmen .....	57

5.2.	Umsetzung des IT-Grundschatzes .....	58
5.3.	Fortschreibungs- und Berichtspflicht .....	58
6.	<b>Glossar .....</b>	<b>60</b>
7.	<b>Literaturverzeichnis .....</b>	<b>65</b>
<b>Anlage A – Technische Infrastruktur .....</b>		<b>1</b>
A.1.	Grundlagen .....	1
A.1.1.	Passive Infrastruktur.....	1
A.1.2.	Technische Vorgaben.....	1
A.1.3.	Auswahl von Standorten für Wiring-Center .....	1
A.2.	Aktive Infrastruktur .....	1
A.2.1.	Campus-Backbone .....	1
A.2.2.	Aktive Komponenten im Bereich der tertiären Vernetzung / Versorgung der Endgeräte.....	1
A.2.3.	Weitere Anschlussvarianten an das Campusnetz .....	1
A.3.	Anbindung an das Internet .....	1
A.4.	Drahtlose Netze (FUNKLAN).....	1

## Versionsstand und Dokumentenstatus

Version	Datum	Status	Bearbeiter
0.5	01. 10. 02	Ersterstellung – Entwurf – Erstellung IT-Grundschutz	AG IT-Sicherheit
0.6	17. 10. 02	Ersterstellung – Entwurf – Ergänzung der Bewertungsmatrix	AG IT-Sicherheit
0.7	14. 01. 03	Ersterstellung – Entwurf – Ergänzung des Kapitels 1.5 Verantwortlichkeiten und Organisation der IT-Sicherheit	CA / IP / AG IT-Sicherheit
0.8	03. 04. 03	Ersterstellung – Entwurf – Fertigstellung des Teilbereichs „IT-Grundschutz“	AG IT-Sicherheit
0.8.1	12. 06. 03	Ersterstellung – Entwurf – Beginn des Kapitel 6 „Risikoanalyse“	DD / AG IT-Sicherheit
0.8.2	07. 08. 03	Ersterstellung – Entwurf – Fertigstellung des Kapitel 1 „IT-Sicherheit an der Freien Universität Berlin“	IP / AG IT-Sicherheit
0.8.3	14. 08. 03	Ersterstellung – Entwurf – Fertigstellung des Kapitel 1 – Ergänzungen/Änderungen von DP	DD / DP
0.8.4	09. 10. 03	Ersterstellung – Entwurf – Fertigstellung des Kapitel 6	DD / AG IT-Sicherheit
0.9	23. 10. 03	Ersterstellung – Entwurf – Fertigstellung des Kapitel 7 und Ersetzen der Bewertungsmatrix durch eine neue Bewertungstabelle	CA / DD / DP / AG IT-Sicherheit
0.9.1	17. 11. 03	Ersterstellung – Entwurf – Änderungen im Kapitel 7 (Seite 46) und einzelner Felder der Bewertungsmatrix	IP / DD / DP / AG IT-Sicherheit
0.9.2	12. 12. 03	Ersterstellung – Entwurf – Ergänzungen in den Grundschutzmaßnahmen	DD / NM
0.9.3	06. 01. 04	Ersterstellung – Entwurf – Neue Gliederung – Änderungen in Kapitel 5 und 6 – Ergänzungen in allen Teilen	DD / NM
0.9.4	12. 01. 04	Ersterstellung – Entwurf – Überarbeitung hinsichtlich von grammatikalischen und Rechtschreibfehlern – Abgleich mit der Organisationsrichtlinie der FU	DD / CA
0.9.5	22. 01. 04	Ersterstellung – Entwurf – Überarbeitung des gesamten Konzepts	AG IT-Sicherheit / DD
0.9.6	04. 01. 04	Ersterstellung – Entwurf – Ergänzungen in den Grundschutzmaßnahmen	DD / CA
0.9.7	15. 03. 04	Ersterstellung – Entwurf – Ergänzungen Kapitel 2 und 3	FT / IC / DD
0.9.8	18. 03. 04	Ersterstellung – Entwurf – Festlegung der letzten Bearbeitungsschritte zu Kapitel 2, 3 und 4	AG IT-Sicherheit
0.9.9	25. 03. 04	Ersterstellung – Entwurf – Überarbeitung zu Kapitel C	FT / DD / NM
1.0	31. 03. 04	Ersterstellung – Entwurf – Überarbeitung zu Kapitel B	HS / DD / NM
1.1	16. 08. 04	Teilweise Berücksichtigung der Anmerkungen von Hr. Sabisch	CA / DD
1.2	10. 11. 04	Anpassungen an die IT-Organisationsrichtlinie	DD
1.3	16. 12. 04	Teilweise Berücksichtigung von Anmerkungen von Hr. Schmidt	DD / CA
1.4	04. 03. 05	Teilweise Berücksichtigung der Anmerkungen der IT-Leiter	DD / NM
1.5	18. 03. 05	Teilweise Einarbeitung der Anmerkungen von Prof. Naumann	DD / NM
1.6	31. 03. 05	Teilweise Einarbeitung der Anmerkungen von Prof. Naumann	DD / NM
1.7	07. 04. 05	Überarbeitung – Workshop der IT-Leiter	NA / TP / HS / WM / DD
1.8	29. 04. 05	Entfernen des Anhangs B	DD
1.9	03. 05. 05	Umbenennung in -richtlinie und kleinere Korrekturen	DD / HS

### Kürzel der Bearbeiter:

NA – Hr. Dr. N. Apostolopoulos  
 CA – Hr. C. Arndt  
 HB – Hr. Dr. H. Busse  
 IC – Hr. I. Camphausen  
 DD – Hr. D. Dräger  
 NM – Fr. N. Manzke  
 UN – Prof. Dr. U. Naumann

IP – Fr. I. Pahlen-Brandt  
 DP – Hr. Dr. D. Pape  
 TP – Hr. T. Prill  
 HS – Hr. H. Scheelken  
 HS – Hr. H. Schmidt  
 FT – Hr. F. Tietz  
 MW – Hr. M. Wilmes

## 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.

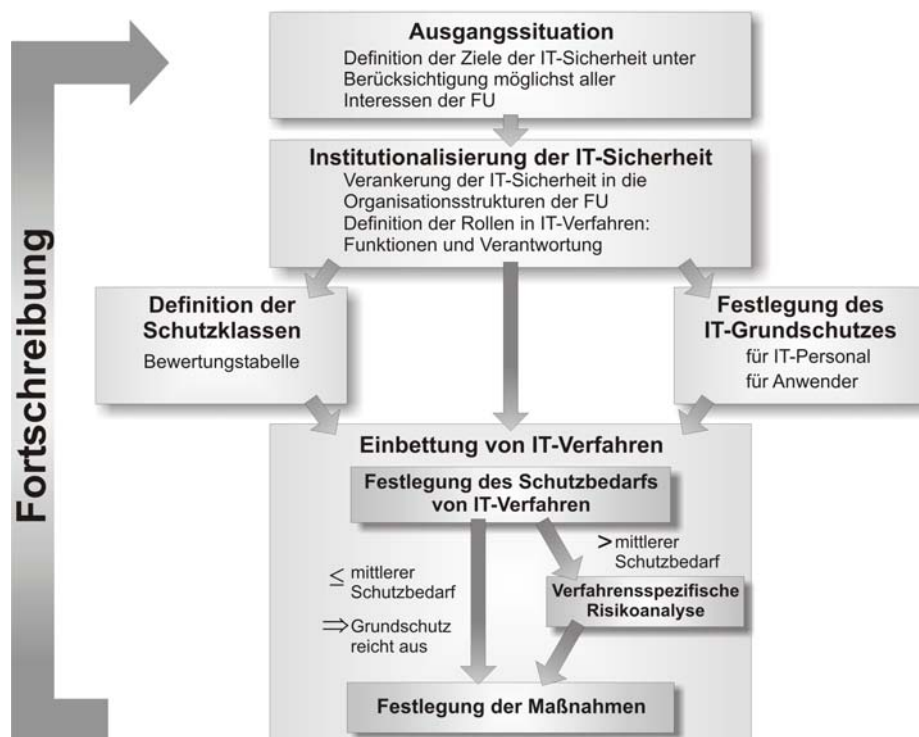


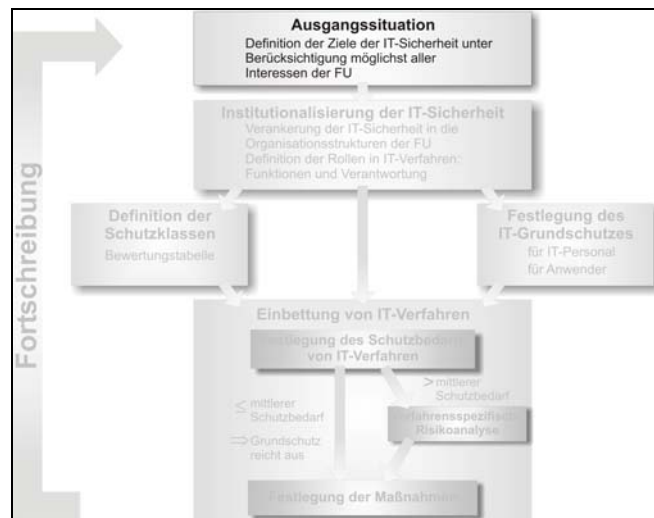
Abbildung 1: Modell des IT-Sicherheitsprozesses

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-Sicherheitsrahmenrichtlinie beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind für die zentrale Universitätsverwaltung und die dezentralen Verwaltungen der Freien Universität Berlin verbindlich. Für den Bereich Forschung und Lehre dagegen hat dieses Dokument noch einen empfehlenden Charakter. Die schrittweise Herstellung der Verbindlichkeit für den Bereich Forschung und Lehre ist eng verbunden mit der Evaluierung der Regelungen hinsichtlich der Anwendbarkeit im Wissenschaftsbetrieb. Der Evaluationsprozess muss in enger Abstimmung und Zusammenarbeit mit den IT-Verantwortlichen der Fachbereiche, Zentralen Einrichtungen und Institute erfolgen.

In diesem Dokument wird die Formulierung „Bereiche“ 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.

# 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 Da-



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

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

Die IT-Sicherheitsrahmenrichtlinie 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-Sicherheitsrahmenrichtlinie verbindlich beschrieben.

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

Die Beschreibung aller IT-Verfahren (siehe 1.2) ist ein notwendiger Bestandteil der IT-Sicherheitsrahmenrichtlinie. 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 Teil 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 verfahrensbezogene Maßnahmen erarbeitet werden, die aus entsprechenden Risikoanalysen abgeleitet werden.

Wegen des stetigen Fortschritts auf dem Gebiet der Informationstechnik muss die IT-Sicherheitsrahmenrichtlinie regelmäßig überprüft und neuen Anforderungen angepasst werden. Für die Umsetzung der IT-Sicherheitsrahmenrichtlinie 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-Sicherheitsrahmenrichtlinie

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

- **IT-Verfahren**

Ein IT-Verfahren besteht aus Arbeitsabläufen und -prozessen, die sich auf IT stützen. Sie bilden eine arbeitsorganisatorisch abgeschlossene Einheit.

- **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 nachvollzogen werden kann, wie und wann welche Daten in das IT- System gelangt sind.

- **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

Ein IT-Verfahren besteht aus IT-gestützten Arbeitsabläufen, die eine arbeitsorganisatorisch abgeschlossene Einheit 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 Sechseck soll ein IT-Verfahren symbolisieren. Alle IT-Verfahren würden den gesamten IT-Einsatz in der Freien Universität Berlin darstellen. (Die Anordnung der Verfahren ist willkürlich gewählt und stellt nicht die Schnittstellen der Verfahren untereinander dar.)

Zu den unverzichtbaren Bestandteilen einer Verfahrensbeschreibung gehören:

- die Aufgabe des Verfahrens,
- ein Mengengerüst,

- eine Beschreibung der zu bearbeitenden Daten,
- eine Auflistung aller Schnittstellen zu anderen Verfahren,
- die eingesetzte Systemtechnik,
- die Rollenverteilung (Arbeitsabläufe),
- ein Schulungskonzept,
- ein Betriebskonzept und
- ein Betreuungskonzept.

Weitere Merkmale eines IT-Verfahrens sind der längerfristige Charakter der erfassten IT-gestützten Arbeitsabläufe. Ein IT-Verfahren wird üblicherweise über mehrere Jahre hinweg betrieben. Außerdem ist der finanzielle Wert aller Ressourcen eines IT-Verfahrens in der Regel relativ groß. Daraus folgt, dass ein einzelner computergestützter Arbeitsplatz im Allgemeinen kein eigenständiges IT-Verfahren darstellt.

Bei der Festlegung eines IT-Verfahrens soll der Grundsatz der Generalisierung bzw. der Zusammenfassung beachtet werden. Es sollten also möglichst viele Arbeitsabläufe von einem Verfahren abgedeckt werden. Beispielsweise können alle IT-gestützten Arbeitsabläufe einer Fachbereichsverwaltung zu einem IT-Verfahren zusammengefasst werden. Normalerweise ist es nicht sinnvoll, einzelne Arbeitsabläufe, wie z.B. die Erledigung der Korrespondenz, als ein eigenes IT-Verfahren festzulegen. Dadurch würde eine große Zahl von IT-Verfahren entstehen, deren strukturierte Bearbeitung kaum mehr leistbar ist. Allerdings gibt es auch gute Gründe, die für eine Trennung von IT-gestützten Arbeitsprozessen sprechen können. Als Anhaltspunkt für eine Zusammenfassung oder eine Trennung von Arbeitsabläufen können u. a. folgende Kriterien dienen:

<b>Trennkriterien</b>	<b>Zusammenfassungskriterien</b>
<ul style="list-style-type: none"><li>• unterschiedlicher Schutzbedarf</li><li>• verschiedene Datenkategorien</li><li>• verschiedene „Datenbesitzer“</li></ul>	<ul style="list-style-type: none"><li>• Arbeitersparnis</li><li>• Zusammenhängende Aufgaben</li></ul>

Die Rollenverteilung innerhalb eines IT-Verfahrens orientiert sich am folgenden Rollenmodell. 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. Zum Beispiel kann bei großen und komplexen IT-Verfahren die Rolle des Applikationsbetreuers von mehreren Personen übernommen werden. Andererseits

kann bei kleinen IT-Verfahren diese Rolle von einer Person übernommen werden, die gleichzeitig auch die Rolle eines Anwenderbetreuers und/oder Key-Users ausfüllt.

Die folgende Grafik skizziert die wichtigsten Rollen innerhalb eines IT-Verfahrens. Die ausführlichere Beschreibung aller Rollen im IT-Bereich beinhaltet die IT-Organisationsrichtlinie der Freien Universität Berlin.

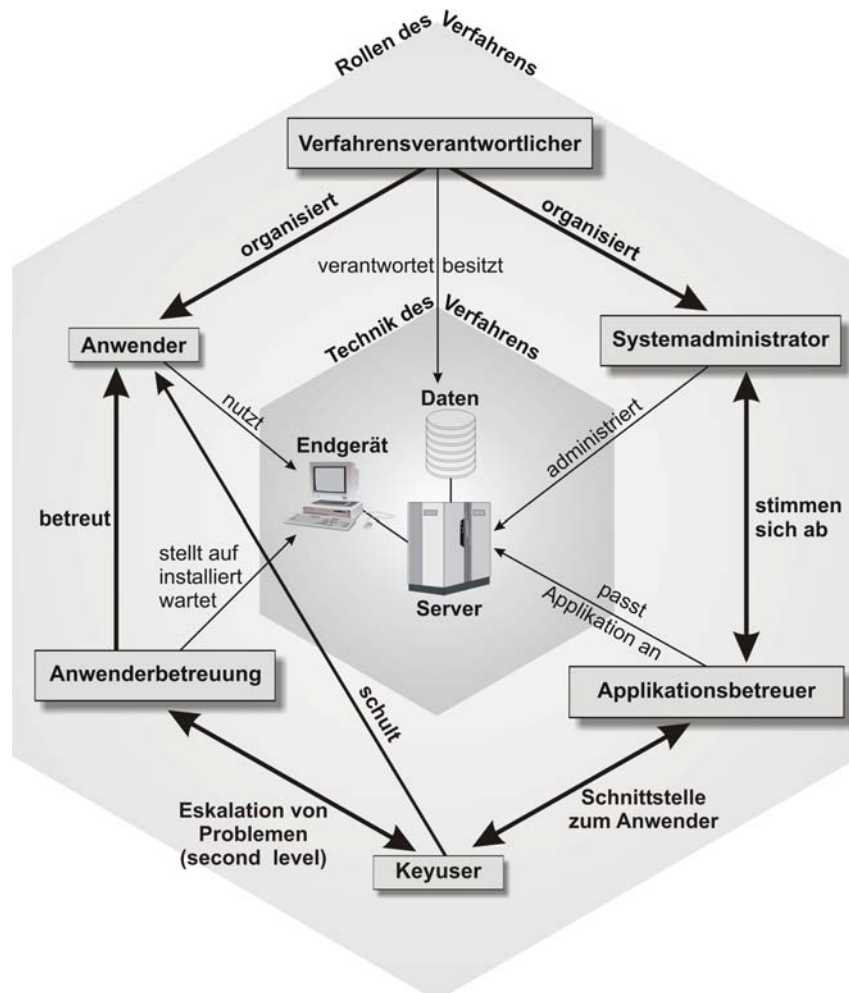


Abbildung 3: Die wichtigsten Rollen (keine Personen) innerhalb eines IT-Verfahrens werden symbolisch dargestellt. Dabei ist zu beachten, dass eine Rolle von einer oder mehreren Personen (Organisationseinheiten) ausgefüllt werden kann. Andererseits kann aber auch eine Person mehrere Rollen wahrnehmen. (Rollen mit verfahrensübergreifender Bedeutung sind hier nicht dargestellt.)

### 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 Bereiche durch ein übergreifendes Campusnetz kann zur Folge haben, dass Sicherheitsmängel in einem Bereich sich auf die Sicherheit von IT-Systemen in einem anderen Bereich der Freien Universität auswirken. Auch aus diesem



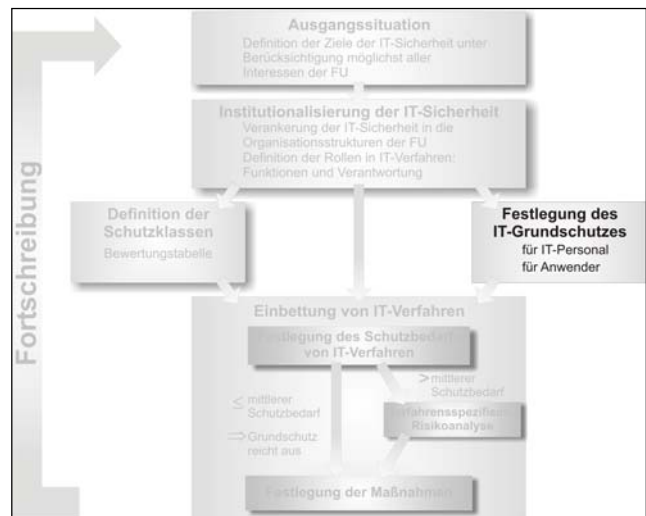
Grunde ist die Gewährleistung der IT-Sicherheit eine Querschnittsaufgabe der gesamten Universität. Sie erfordert über die Einhaltung der in dieser IT-Sicherheitsrahmenrichtlinie aufgestellten Regeln hinaus die aktive Mitarbeit aller beteiligten Personen – und zwar hierarchie- und bereichsübergreifend.

Alle Rollen im IT-Bereich und damit auch die Rollen bezüglich der IT-Sicherheit sind in der IT-Organisationsrichtlinie der Freien Universität Berlin beschrieben.

## 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 zu erreichen, die die Bereiche Organisation, Personal, Infrastruktur, Hard- und Software, Kommunikation und Notfallvorsorge betreffen.

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 niedrigem bis mittlerem Schutzbedarf. Sie bilden die Grundlage für alle IT-Verfahren der Freien Universität Berlin. Ihre Realisierung in den Bereichen wird mittelfristig Voraussetzung für die Teilnahme an übergreifenden IT-Verfahren wie der Nutzung zentraler Dienste durch die Bereiche sein, z.B. E-Mail, Internet, Datensicherung sein.

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 eines einzeln betriebenen Rechners ohne Sicht auf die Folgen für das vernetzte Gesamtsystem erscheinen die beschriebenen Maßnahmen für die Mitarbeiter möglicherweise unbequem und übertrieben. Die zahlreichen sicherheitsrelevanten Vorfälle in der jüngeren Vergangenheit unterstreichen jedoch stark ihre Notwendigkeit. Beispielsweise kann die Verbreitung von Netzwürmern, E-Mail-Viren und Trojanischen Pferden über längst bekannte Sicherheitslücken eingesetzter Standardprogramme durch aktuelle Virens Scanner und entsprechende Programmaktualisierung verhindert werden.

Ein durchdachtes Server- und Datensicherungskonzept kann wirksam vor den Folgen von Diebstählen von Rechneranlagen aus schlecht gesicherten Gebäuden und



dem damit einhergehenden unwiederbringlichen Verlust von wichtigen Daten schützen. Eine gute und klar strukturierte Organisation kann dazu führen, dass wichtige Informationen z.B. über Sicherheitslücken oder Missbrauch von Rechnern zeitnah an die Endanwender weitergeleitet werden können. So können Schäden und Kosten vermieden werden, die sonst die Mitarbeiter zusätzlich belasten würden.

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-Sicherheitsrahmenrichtlinie“).

Die Maßnahmen des Grundschutzes werden gesondert für IT-Anwender und IT-Personal dargestellt. Der Maßnahmenkatalog wird zukünftig allen Anwendern an der Freien Universität Berlin ausgehändigt werden. Die Maßnahmen des Grundschutzes für IT-Personal wenden sich unter anderem an IT-Betreuer und Systemadministratoren, die hier Vorgaben für ihre Arbeit finden.

Als Basis für die hier dargestellten IT-Grundschutzmaßnahmen diene das IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik. Die dort beschriebenen Maßnahmen wurden den Besonderheiten der Freien Universität Berlin angepasst. Bei Fragen zu einzelnen Maßnahmen werden die detaillierteren Ausführungen im IT-Grundschutzhandbuch empfohlen.

Zu jeder Regel und zu jeder Maßnahme sind, um eindeutige Verantwortlichkeiten festzulegen, Verantwortliche für die Initiierung und Verantwortliche für die Umsetzung konkret benannt. Grundlage allen Handelns für diese Verantwortlichen sind die in diesem Kapitel beschriebenen Maßnahmen des IT-Grundschutzes. Bei der Initiierung muss unterschieden werden zwischen dem bereichsweise zuständigen IT-Verantwortlichen und dem Verfahrensverantwortlichen.

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



## 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 mit 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. Jeder schwerwiegende Vorfall ist zu dokumentieren.

### 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:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	Dienststelle Arbeitssicherheit

Alle Maßnahmen und Einrichtungen, die dem vorbeugenden Brandschutz dienen, sind einzuhalten. Lüftungsöffnungen an den Geräten dürfen nicht verstellt oder verdeckt werden. In allen Räumen, in denen Server und Netzwerkkomponenten untergebracht sind, besteht Rauchverbot.

- **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, 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 ein Bereich eine pauschale Freigabe für Teilbereiche festgelegt hat. Rechnersysteme sind gegen das unbefugte Herunterladen hard- und softwaretechnisch zu schützen.

- **Keine private Hard- und Software (M1.7)**

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

Die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der Freien Universität Berlin und deren Netzen ist nicht gestattet. Sondergenehmigungen, zum Beispiel im Rahmen von Schulungsveranstaltungen oder Vorträgen, können auf Antrag durch die zuständigen IT-Verantwortlichen des Bereichs oder dafür zuständiges IT-Personal erteilt werden. Ausgenommen von dieser Regelung sind speziell für den Einsatz privater Computer gekennzeichnete Bereiche, wie zum Beispiel in Bibliotheken.

- **Virenschutz (M1.8)**

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

Auf allen Arbeitsplatz-PCs ist, soweit technisch möglich, 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.

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.

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

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

Alle Rechnersysteme sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst 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.

- **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.

Für die Wahl von Passwörtern werden folgende Regeln dringend empfohlen:

- 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 werden sollte, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem zuständigen Vorgesetzten und dem IT-Personal zu melden. (Siehe M1.3)

Vergisst ein Benutzer sein Passwort, hat er beim Administrator ohne vorheriges Ausprobieren das Zurücksetzen zu veranlassen. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird.

- **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 Bereichen 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 des Bereichs 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 müssen 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 Bereichen 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

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 erstmaligen und 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

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 Behälter 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.

Aussondernde 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. (Siehe auch M1.16)

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

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

Papiere mit vertraulichem Inhalt (auch Testausdrucke) 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-, 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 Maß-

nahmen 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. Zu den unverzichtbaren Bestandteilen einer Verfahrensbeschreibung gehören:

- Aufgabe des Verfahrens
- Datenbeschreibung
- Schnittstellen zu anderen Verfahren
- Systemtechnik
- Zuordnung von Personen zu Rollen (entsprechend dem Rollenmodell)

Siehe auch 1.2 IT-Verfahren.



- **Rollentrennung (M2.4)**

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

Für jedes IT-Verfahren 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.

Siehe auch 1.2 IT-Verfahren.

- **IT-Verantwortlicher (M2.5)**

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

Den IT-Verantwortlichen der Bereiche kommt im Rahmen des Sicherheitsrahmenkonzeptes der FU 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 den Bereich ihrer Zuständigkeit. Bei Fragen des IT-Einsatzes sind sie sowohl Ansprechpartner für die Mitarbeiter ihres Bereiches als auch für Dritte (Bereichsfremde).

Eine nähere Beschreibung von Rolle und Aufgaben der 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:

- Vertretungsregelungen, insbesondere im Administrationsbereich
- Zugriffsrechte
- Organisation, Verantwortlichkeit und Durchführung der Datensicherung
- Installation und Freigabe von Software
- Zweck, Freigabe und Einsatz selbsterstellter Programme
- Dienstanweisungen

- Arbeitsanleitungen für Administrationsaufgaben u.ä.
- auftretende Sicherheitsprobleme aller Art
- Notfallregelungen
- Wartungsvereinbarungen
- Verfahrensbeschreibungen nach Datenschutzrecht

Nur dokumentierte Verfahren dürfen betrieben werden. Der IT-Verantwortliche sorgt für die aktuelle Dokumentation der Verfahren seines Bereiches. Der IT-Verantwortliche ist verantwortlich für die Erstellung und Pflege der Dokumentation der Verfahren seines Bereiches. 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, können für die Fortschreibung der IT-Sicherheitsrahmenrichtlinie wertvolle Hinweise liefern. Sie 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.

- **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 dieses Konzepts von den zentralen Dienstleistern unter Maßgabe der vom CIO-Gremium definierten Strategien festzulegen.

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

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

Ein leistungsfähiger Nutzerservice, zentral gesteuerte Datensicherungsmaßnahmen, die Möglichkeit der Ablage von Daten auf zentrale Fileserver 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.

- **Sicherung der Netze innerhalb der Freien Universität Berlin (M2.11)**

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

Da für die Bereitstellung zentraler Serviceleistungen der Ausbau der Vernetzung voran zu treiben ist, ist für sensible Bereiche dabei die Möglichkeit der Nutzung von Applikationsservern und laufwerkslosen Arbeitsplatzrechnern bzw. Terminals zu prüfen. Gegebenenfalls sind vorhandene Wechsellaufwerke (z.B. Disketten-, CD-ROM-Laufwerke) zu deaktivieren.

- **Revision der Sicherheit (M2.12)**

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 besonderer Wert zu legen. (Zum Beispiel wäre es sinnvoll, nur Anbieter mit Zertifikaten des BSI in Betracht zu ziehen.)

### 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.

Kurzzeitig befristet beschäftigte Mitarbeiter (Beschäftigungsverhältnis von weniger als einem Jahr) sollten nach Möglichkeit keine Aufgaben übernehmen, die nur mit Administratorrechten ausgeführt werden können.

- **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. 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 im System abgebildet sein und darf nicht durch die Weitergabe von Passwörtern erfolgen.

Vertretungsrechte sollten im System 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 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 (öffentlicher zugänglicher Bereich, Lage zur Straße usw.) sind besondere bauliche Maßnahmen, wie

zum Beispiel einbruchssichere Fenster, einbruchssichere Türen, Bewegungsmelder o. ä. zur Verhinderung von gewaltsamen Eindringen 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 erfordert. 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 internen oder vertraulichen Inhalt nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

- **Sicherung der Netzknoten (M2.19)**

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 (M2.20)**

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

Die Verkabelung des LAN ist klar zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Administratoren müssen einen vollständigen Überblick

über die Kabelverlegung und die Anschlussbelegung zentraler Komponenten haben. Nicht benutzte Anschlüsse sollen abgeklemmt oder deaktiviert werden. Erweiterungen und Veränderungen an der Gebäudeverkabelung, auch die Inbetriebnahme von Funknetzen, sind mit den IT-Verantwortlichen des eigenen Bereichs und mit dem Hochschulrechenzentrum abzustimmen.

- **Geschützte Kabelverlegung (M2.21)**

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.

- **Einweisung und Beaufsichtigung von Fremdpersonal (M2.22)**

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	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 bzw. untersagt 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 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 (M2.23)**

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.



- **USV (M2.24)**

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 (M2.25)**

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

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 Materialien 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 TF30 und TF90 zu nennen. Außerdem sind Brandmelder und Handfeuerlöscher (Brandklasse B, CO<sub>2</sub>-Löscher) vorzusehen. Für Hinweise und eingehende Beratung wenden Sie sich an Ihren örtlichen Brandschutzbeauftragten.

- **Schutz vor Wasserschäden (M2.26)**

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

IT-Systeme, die wichtige oder unverzichtbare Komponenten zur Aufrechterhaltung eines geordneten Betriebes sind, 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.



## 2.2.5. Hard- und Softwareeinsatz

- **Beschaffung, Softwareentwicklung (M2.27)**

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

Die Beschaffung von Soft- und Hardware 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 Bereichen durchgeführt.

- **Kontrollierter Softwareeinsatz (M2.28)**

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 ein Bereich eine pauschale Freigabe für Teilbereiche festgelegt hat. Rechnersysteme sind gegen das unbefugte Herunterladen hard- und softwaretechnisch zu schützen.

- **Separate Entwicklungsumgebung (M2.29)**

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 (M2.30)**

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 (M2.31)**

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

Softwareentwicklungen ab einer gewissen Größenordnung, die in der Projekt-richtlinie beschrieben sind, müssen nach standardisierten Verfahren und nach Maßgabe der für die Universität geltenden Regelungen durchgeführt werden, die u. a. ein klar umrissenes Projektmanagement und eine Qualitätssicherung beinhalten.

- **Schutz vor Schadprogrammen (M2.32)**

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

Auf allen Arbeitsplatz-PCs ist, soweit möglich, ein aktueller Virens Scanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Jeder Bereich 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.

- **Diskettenlose PCs (M2.33)**

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

Bei erhöhtem Schutzbedarf müssen alle äußeren Zugänge des PCs (zum Beispiel Disketten- und CD-ROM-Laufwerke) gesperrt werden, wenn sie für die zu erledigenden Aufgaben nicht notwendig sind. Der Zugriff auf das Rechner-BIOS ist durch ein Passwort zu schützen.

- **Dokumentation (M2.34)**

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 (M2.35)**

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

Maßnahmen zur Ausfallsicherheit sind entsprechend der jeweiligen Anforderung 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 Diebstahl-Sicherungen (M2.36)**

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 die 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.

- **Netzzugänge (M2.37)**

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 des Bereichs und ggf. mit dem Datenschutzbeauftragten ist unzulässig.

- **Personenbezogene Kennungen (Authentisierung) (M2.38)**

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 geregelten Verfahren erfolgen. Die Einrichtung und Freigabe sind zu dokumentieren.

- **Administratorkennungen (M2.39)**

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 (M2.40)**

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

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass der zuständige IT-Verantwortliche rechtzeitig über das Ausscheiden oder den Wechsel eines Mitarbeiters informiert wird. Der zuständige Bereich 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, 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 (M2.41)**

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 dreifacher fehlerhafter Passworteingabe muss eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann.
- 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) (M2.42)**

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 Bereichen 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 Zugangsbegrenzung auf die notwendigen Rechner (i.d.R. sind es der betreffende Server und die Arbeitsplatz-PCs) zu begrenzen. Es ist ebenfalls zu prüfen, inwieweit die Zugangserlaubnis auf bestimmte Zeiten begrenzt werden kann. Beispielsweise könnte der Zugang zu wichtigen Systemen für die Anwender auf die üblichen Arbeitszeiten eingeschränkt werden.

- **Änderung der Zugriffsrechte (M2.43)**

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 (M2.44)**

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. Bei längerem Verlassen des Raumes 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. 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. Die hier skizzierten technischen und organisatorischen Lösungen werden in einem gesonderten IT-Revisionskonzept beschrieben.

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.

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 auf den Servern (M2.45)**

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 wurde. Das Prinzip der Zweckbindung nach § 11 (5) BlnDSG ist unbedingt zu beachten.

- **Protokollierung durch Anwendungsprogramme (M2.46)**

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

Bei der Protokollierung durch Anwendungssysteme ist der Grundsatz der Datenvermeidung § 5a BlnDSG zu beachten, d.h. es sind so wenig personenbezogene Daten wie möglich zu protokollieren. Von Anwendungssystemen erzeugte Protokolldaten sind vor dem Zugriff Unbefugter zu schützen. Es gelten die oben genannten Regeln (M2.46) entsprechend, insbesondere ist bei Daten mit Personenbezug das Zweckbindungsgebot § 11 (5) BlnDSG zu beachten.

- **Protokollierung der Administrationstätigkeit (M 2.47)**

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 Risiken und Gefahren der elektronischen Kommunikation und der Datenübermittlung in Kenntnis zu setzen.

- **Sichere Netzwerkadministration (M2.48)**

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 (M2.49)**

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 (M2.50)**

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 (M2.51)**

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 ist 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 (M2.52)**

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 (M2.53)**

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 (M2.54)**

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 (M2.55)**

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

Die Sicherung der Daten auf Servern sollte im angemessenen Rhythmus erfolgen. Auch System- und Programmdateien sind nach Veränderungen zu sichern. 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 (M2.56)**

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 (M2.57)**

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

Die Sicherungsdatenträger sind getrennt vom jeweiligen Rechner aufzubewahren. Bei Datenbeständen ab Schutzklasse „niedrig bis mittel“ 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 (M2.58)**

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

Alle Datenträger sind soweit möglich eindeutig zu kennzeichnen. Aus der Beschriftung soll die Verwendung (Verfahren, Dateien, Inhalt), Datum der ersten Ingebrauchnahme sowie das Datum des erstmaligen und 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 (M2.59)**

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 (M2.60)**

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 (M2.61)**

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 FU- fremde 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 Ausnahmefällen 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.

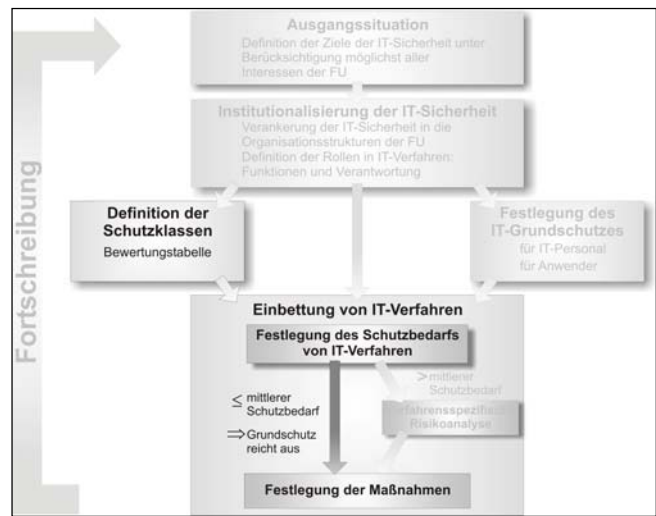
- **Sichere Entsorgung vertraulicher Papiere (M2.62)**

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

IT-Sicherheitsmaßnahmen müssen sich grundsätzlich aus den Sicherheitsanforderungen der Anwender ableiten lassen. Dieser Grundsatz entspringt der Überlegung, dass die eingesetzte Informationstechnik vorrangig nicht aus sich heraus schützenswert ist, sondern vielmehr wegen ihres Wertes für die Anwender. Der Wert der Daten und Funktionen, die die IT bereitstellt, ist in der Regel um ein vielfaches höher als der Wert der Technik selbst. Andernfalls wäre die Beschaffung der IT gar nicht zu rechtfertigen.



Deswegen muss am Beginn eines IT-Sicherheitskonzepts die Analyse der Sicherheitsanforderungen der Anwender stehen. Diese Anforderungen werden ermittelt in Bezug auf die drei Grundbedrohungen Verlust der Verfügbarkeit (Verfg.), Verlust der Integrität (Integ.) und Verlust der Vertraulichkeit (Vertr.).

Dessen ungeachtet muss für jedes IT-Verfahren ein Mindestmaß an Sicherheit gewährleistet werden. Daher sind die Regeln des IT-Grundschutzes (Kapitel 2 „Definition des Grundschutzes“) immer anzuwenden, unabhängig von dem Ergebnis der Schutzbedarfsanalyse.

In Anlehnung an das IT-Sicherheitshandbuch des BSI und die einschlägigen Empfehlungen der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) wurde für die Freie Universität Berlin eine Bewertungstabelle für die Sicherheitsanforderungen (Schutzbedarf) aufgestellt und abgestimmt (Tabelle 1: Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren). Dieser Bewertungsmaßstab klassifiziert den Schutzbedarf in drei Werte (Schutzklassen) „niedrig bis mittel“, „hoch“ und „sehr hoch“ und beschreibt die Bedeutung dieser Werte in Hinblick auf verschiedene Kriterien. Dieses Bewertungsverfahren bildet die Grundlage für eine einheitliche Beurteilung des Schutzbedarfs der verschiedenen IT-Verfahren, die von der Freien Universität Berlin projektiert und betrieben werden.



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 andere Gesetze und Vorschriften	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 Aufgabenerfüllung in einem Teilbereich ein	... gefährdet den Auftrag der gesamten Universität
	Verfg.	Verlust der Daten ...			
Negative Außenwirkung	Vertr.	Missbrauch der Daten ...	... führt maximal zum Ansehensverlust eines Teilbereichs gegenüber der restlichen FU oder bei einer eingeschränkten Öffentlichkeit	... führt zu einem Ansehensverlust der FU oder eines Teilbereichs bei einer eingeschränkten Öffentlichkeit	... 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 <125.000 €	Summe der finanziellen Auswirkungen < 5.000.000 €	Summe der finanziellen Auswirkungen >= 5.000.000 €
	Integ.	Unberechtigte Manipulation der Daten			
	Verfg.	Verlust der Daten			
daraus resultierender Schutzbedarf:			niedrig bis mittel	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“.



Der Schutzbedarf kann mit Hilfe der Bewertungstabelle ermittelt werden. Für jede einzelne Beeinträchtigungskategorie wird

1. die Art der möglichen Bedrohungen betrachtet,
2. die dazu korrespondierende Abschätzung des maximal möglichen Schadens in der betreffenden Spalte getroffen,
3. der resultierende Schutzbedarf je Kategorie/Bedrohung am Fuß der Tabelle ermittelt.

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

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:			niedrig bis mittel	hoch	sehr hoch

Tabelle 2: Beispiel-Ergebnis einer Schutzbedarfsbestimmung.

Wird der Schutzbedarf in der Schutzklasse „niedrig bis mittel“ eingestuft, reichen im Allgemeinen die Maßnahmen des IT-Grundschatzes aus. In allen anderen Fällen, also wenn das IT-Verfahren in die Schutzklasse „hoch“ oder „sehr hoch“ eingestuft wird, muss eine verfahrensspezifische 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 darstellen.

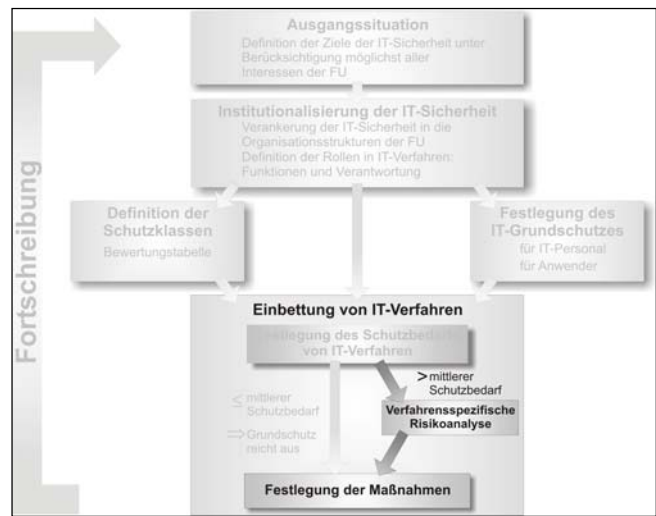


Abbildung 4: Vereinfachte Darstellung der Schutzbedarfsanalyse und der sich daraus ergebenden Konsequenzen.

Die Dokumentation der Schutzbedarfsanalyse besteht im Allgemeinen nicht nur aus dem Ergebnis der Bewertungstabelle, sondern umfasst noch weitere notwendige Angaben über 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 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 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 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 47) 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 K Co IT, erfolgen.

Die Durchführung der 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 47) 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 3: 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 4. 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	niedrig bis mittel 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 4: Risikoklassen

Zusammenfassend sind folgende Schritte für die Risikoanalyse durchzuführen:

Schritt 1: Erfassung der für das IT-Verfahren relevanten und bedrohten Objekte

Hilfsmittel: Sicherheitshandbuch des BSI [Sicherheitshandbuch, Anhang 3]

Schritt 2: Bewertung des Schutzbedarfs der Objekte

Hilfsmittel: Bewertungsmatrix (Seite 47)

Schritt 3: Bestimmung der Häufigkeit von Schäden

Hilfsmittel: Tabelle der Häufigkeitswerte (Seite 51)

Schritt 4: Zusammenstellung und Bewertung (Klassifizierung) der Risiken

Hilfsmittel: Tabelle der Risikoklassen (Seite 52)

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 ausführlichere 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 verfahrensspezifische Bedrohungen und Bewertungen, sowie ggf. geeignete Maßnahmen zur Risikoreduzierung ausgearbeitet werden.

(Hinweis: Die Beispieltabelle erstreckt sich über die folgenden drei Seiten).

Bezeichnung der Bedrohung	Grundbedrohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenswert	Häufigkeit	Risikoklasse	Maßnahmen
<b>– Hardware –</b>						
Technisches Versagen	Verfügb.	Produktivsystem, PDC	3	sehr selten	Untragbar	M-01: Wartungsvertrag Produktivsystem und PDC
	Verfügb.	Weitere Server	2	sehr selten	Tragbar	M-02: Wartungsvertrag weitere Server
	Verfügb.	Arbeitsplatz-PCs	1	selten	Tragbar	
	Verfügb.	Drucker	1	selten	Tragbar	
	Verfügb.	Zentrale Netzwerkkomponenten	1	selten	Tragbar	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Diebstahl	Verfügb. Vertraul.	Server	2	selten	Untragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude M-14: Zugriffsschutz Server
Spannungsschwankungen, Blitzschlag	Verfügb.	Produktivsystem, PDC	2	sehr selten	Tragbar	M-07: Unterbrechungsfreie Stromversorgung
	Verfügb.	Weitere Server	1	sehr selten	Tragbar	M-07: Unterbrechungsfreie Stromversorgung
Fehlbedienung	Vertraul. Integrit.		1	sehr selten	Tragbar	
Sabotage	Verfügb.	Produktivsystem, PDC	1	sehr selten	Tragbar	
	Verfügb.	Weitere Server	1	sehr selten	Tragbar	
Unkontrollierter Zugang	Verfügb. Integrit. Vertraul.	Zentrale Server	2	selten	Untragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude M-14: Zugriffsschutz Server
	Integrit. Vertraul.	Clients	1	selten	Tragbar	M-08: Zugangsschutz Clients
<b>– Infrastruktur –</b>						
Höhere Gewalt, Terror, Vandalismus	Verfügb.	Serverraum	1	praktisch nie	Tragbar	
	Verfügb.	Zentrale Netzkomponenten	1	sehr selten	Tragbar	
Feuer	Verfügb.	Serverraum	1	sehr selten	Tragbar	
	Verfügb.	Netzkomponenten	1	sehr selten	Tragbar	
Wasser	Verfügb.	Serverraum	1	sehr selten	Tragbar	
	Verfügb.	Netzkomponenten	1	sehr selten	Tragbar	

Bezeichnung der Bedrohung	Grundbedrohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenswert	Häufigkeit	Risikoklasse	Maßnahmen
Überhitzung	Verfügb.	Serverraum	1	öfter	Untragbar	M-09: Klimatisierung
Ausfall der Stromversorgung	Verfügb.	Zentrale Hardware	1	sehr selten	Tragbar	M-07: Unterbrechungsfreie Stromversorgung
Unbefugter Zugang	Vertraul.	Serverraum	2	sehr selten	Tragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude
	Vertraul.	Arbeitsräume	1	selten	Tragbar	M-10: Nicht öffentliche Räume
<b>– Kommunikation –</b>						
Ausfall	Verfügb.	Netzwerk	2	sehr selten	Tragbar	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Überlastung	Verfügb.	Netzwerk	1	selten	Tragbar	
Abhören	Vertraul.	Netzwerk	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung
Manipulation	Vertraul. Integrit.	Netzwerk	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung
Anschließen zusätzlicher Endgeräte	Vertraul. Integrit.	Personenbezogene Daten	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Zugangsschutz Netzkomponenten
Unerlaubter Zugang	Vertraul. Integrit.	Netzwerk	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung
<b>– Datenträger –</b>						
Unkontrollierter Zugriff	Verfügb. Integrit. Vertraul.	Sicherungsbänder	2	sehr selten	Tragbar	M-12: Verschlüsselung der Datensicherung, Zugangsschutz
Beschädigung	Verfügb. Integrit.	Sicherungsbänder	1	sehr selten	Tragbar	
	Verfügb. Integrit.	Festplatten	1	sehr selten	Tragbar	M-13: RAID-5-System, Spiegelplatten
Fehlerhafte Erzeugung	Verfügb. Integrit.	Datenträger	1	sehr selten	Tragbar	
Unzureichende Entsorgung	Vertraul.	Datenträger	2	praktisch nie	Tragbar	
Diebstahl	Verfügb. Vertraul.	Datenträger	2	sehr selten	Tragbar	M-12: Verschlüsselung der Datensicherung, Zugangsschutz
<b>– Software, Daten –</b>						
Unerlaubtes Aufspielen von Software	Verfügb.	Software, Daten	1	sehr selten	Tragbar	M-14: Zugriffsschutz Server
Fehlbedienung	Verfügb. Integrit. Vertraul.	Betriebssystem, Datenbank	1	sehr selten	Tragbar	
Unerlaubter Zugriff und Einblick	Integrit. Vertraul.	Datenbank, Daten, Passwörter	2	sehr selten	Tragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude M-14: Zugriffsschutz Server



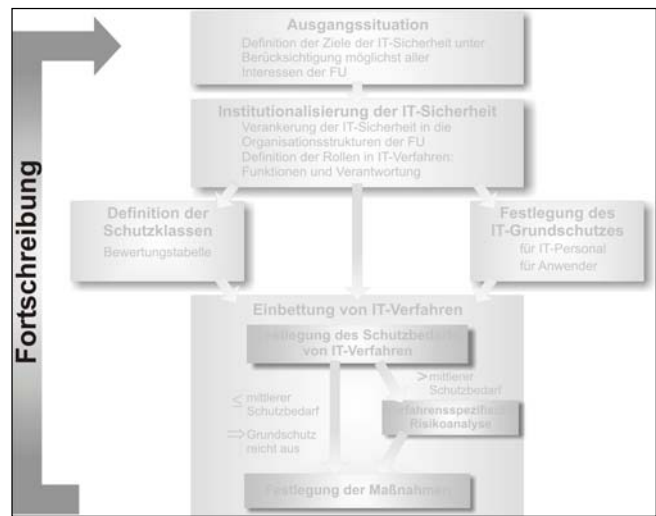
Bezeichnung der Bedrohung	Grundbedrohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenswert	Häufigkeit	Risikoklasse	Maßnahmen
Mangelhafte Verwaltung der Zugriffsrechte	Integrit. Vertraul.	Datenbank	2	selten	Untragbar	M-15: Rollentrennung
Schadprogramme (Computerviren)	Verfügb. Integrit.	Betriebssystem	1	sehr selten	Tragbar	
	Vertraul. Integrit.	Clients	1	öfter	Untragbar	M-16: Virens Scanner
<b>– Papier –</b>						
Unvollständigkeit, mangelnde Aktualität	Verfügb.	Systemdokumentation	1	sehr selten	Tragbar	
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Tragbar	
Unzureichende Entsorgung	Vertraul.	Systemdokumentation	1	sehr selten	Tragbar	
	Vertraul.	Personenbezogene Daten	2	selten	Untragbar	M-17: Schredder
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Tragbar	
<b>– Personen –</b>						
Ausfall	Verfügb.	Administratoren, Applikationsbetreuer	2	sehr selten	Tragbar	M-18: Vertretung
Unkenntnis	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer	1	sehr selten	Tragbar	
	Integrit. Vertraul.	Anwender	1	sehr selten	Tragbar	
Überlastung	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer	2	sehr selten	Tragbar	M-15: Rollentrennung M-18: Vertretung
	Integrit. Vertraul.	Anwender	1	sehr selten	Tragbar	
Fehlende Kontrollen und Regelungen	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer	2	sehr selten	Tragbar	M-19: Kontrolle der Akteure
	Integrit. Vertraul.	Anwender	2	sehr selten	Tragbar	M-19: Kontrolle der Akteure
Nachlässige Passworthandhabung	Vertraul.	Passwörter	2	sehr selten	Tragbar	M-20: Festlegung der Passwortregeln
Kriminelle Absicht	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer, Anwender	2	sehr selten	Tragbar	M-15: Rollentrennung M-21: Kontrolle der Protokoll-Dateien
	Verfügb. Integrit. Vertraul.	Externe	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung M-06: Zugangsschutz M-14: Zugriffsschutz

Tabelle 5: 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.

## 5. Umsetzung der IT-Sicherheitsrahmenrichtlinie

Aufgrund der hohen Eigenständigkeit der einzelnen Bereiche 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 Bereiche verteilt. Die entscheidenden Impulse sollen dabei von den IT-Verantwortlichen ausgehen.



Die Verbreitung und Umsetzung der IT-Sicherheitsrahmenrichtlinie soll nach folgendem, gemeinsam mit den IT-Verantwortlichen der Bereiche abgesprochenem Vorgehen geschehen.

### 5.1. Publikation der IT-Sicherheitsrahmenrichtlinie, insbesondere der IT-Grundschutzmaßnahmen

- Die IT-Sicherheitsrahmenrichtlinie wird als FU-Rundschreiben an die Bereiche verteilt und ist dann verbindlich.

Verantwortlich: Präsidium	Termin: unverzüglich
---------------------------	----------------------

- Innerhalb der Bereiche ist sicherzustellen, dass alle Mitarbeiter die für sie relevanten Teile der IT-Sicherheitsrahmenrichtlinie 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 verfahrensspezifischen Regelungen

als bekannt voraus gesetzt werden können.

Verantwortlich: Bereichsleiter	Termin: unmittelbar nach Verabschiedung
--------------------------------	---

## 5.2. Umsetzung des IT-Grundschatzes

Die Gesamtverantwortung für die Umsetzung der verfahrensspezifischen Maßnahmen des IT-Grundschatzes liegt in der Regel bei den IT-Verantwortlichen der Bereiche. Sofern ein Bereich einen IT-Sicherheitsbeauftragten benannt hat, liegt die Umsetzung der IT-Grundschutzmaßnahmen in seinem Zuständigkeitsbereich. Bei der Anwendung einzelner Grundschutzmaßnahmen sind die bei jeder Maßnahme angegebenen Verantwortlichkeiten über die Initiierung und Umsetzung zu beachten.

## 5.3. Fortschreibungs- und Berichtspflicht

Die IT-Sicherheitsrahmenrichtlinie bedarf der ständigen Überarbeitung und Weiterentwicklung. Neu hinzukommende IT-Verfahren und IT-Vorhaben müssen ergänzt und Veränderungen in einzelnen Verfahren eingearbeitet werden. Veränderungen in der Bedrohungssituation oder technische Entwicklungen sind zu berücksichtigen. Turnusmäßig (z.B. im Zusammenhang mit der jährlichen Fortschreibung der IT-Sicherheitsrahmenrichtlinie) 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.

Zur Fortschreibung der IT-Sicherheitsrahmenrichtlinie gehören:

- Regelmäßige Aktualisierung der Grundschutzmaßnahmen und der Werkzeuge

Verantwortlich: CIO, IT-Verantwortliche	Turnus: jährlich	Termin: 1. März
--	------------------	-----------------

- Regelmäßige Aktualisierung der Beschreibung der Infrastruktur

Verantwortlich: ZEDAT	Turnus: jährlich	Termin: 1. März
-----------------------	------------------	-----------------

- Beschreibung neuer IT-Verfahren

Verantwortlich: Verfahrensverantwortliche	Turnus: bei Bedarf	Termin: bei Bedarf
---	--------------------	--------------------

- Aktualisierung der Information bereits gemeldeter IT-Verfahren durch
  - Bestätigung des unveränderten Betriebs
  - oder Aktualisierung der Verfahrensbeschreibung
  - oder Meldung der Einstellung eines IT-Verfahrens.

Verantwortlich: Verfahrensverantwortliche, IT-Verantwortliche der Bereiche	Turnus: jährlich	Termin: 1. März
---	------------------	-----------------

Mit der vorliegenden IT-Sicherheitsrahmenrichtlinie 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

### **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. KeyUser, 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 §3BlnDSG

### **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 bestimmten 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)**

Berliner Regelungen zum Schutz personenbezogener Daten, vgl. auch Bundesdatenschutzgesetz (BDSG)

### **Betriebssystem**

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

**BSI**

Bundesamt für Sicherheit in der Informationstechnik des Bundesinnenministeriums ([www.bsi.de](http://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 Originalen noch eine Verfügbarkeit der Daten gewährleistet.

**Datenträger**

Medium zum Speichern der Daten wie Magnetbänder, Festplatte, CDROM oder Diskette

**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 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-Betreuer**

Sorgt operativ für den Betrieb der IT-Systeme in den Organisationseinheiten und ist Ansprechpartner für den Betrieb bereichsübergreifender IT-Verfahren.

Er setzt die Vorgaben des Bereichsverantwortlichen um und hat gute Kenntnisse über die in seiner Organisationseinheit eingesetzten 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, Verfahrensbetreuer, Programmmentwickler, IT-Verfahrensverantwortliche und IT-Bereichsverantwortliche

**IT-Sicherheitsbeauftragter**

verfolgt die vorgegebenen Ziele des Grundschutzes und der vereinbarten Schutzstufe und setzt diese verantwortlich um

**IT-Sicherheitsrahmenrichtlinie**

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-Sicherheitsrahmenkonzept“ gebräuchlich. Der Begriff „Richtlinie“ wurde gewählt, um die Verbindlichkeit der Regelungen und Maßnahmen zu unterstreichen.) 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 FU.

**KBS**

Kassenbewirtschaftungssystem

**Key-User**

besonders geschulte Anwender, die erster 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

**MBS**

Materialbewirtschaftungssystem

**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 Komponenten, 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

**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



**Virens Scanner**

Entsprechende Programme, die in der Lage sind, Schadprogramme zu identifizieren. Wegen der schnellen Entwicklung und Verbreitung neuer Viren ist der Virens Scanner immer auf den 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)

**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>

### **[Grundschutzhandbuch]**

IT-Grundschutzhandbuch, Standardsicherheitsmaßnahmen  
Mai 2002, Schriftenreihe zur IT-Sicherheit – Band 3, BSI,  
Quelle: <http://www.bsi.de/gshb/deutsch/menue.htm>

### **[Daten-Kommunikationsverbindungen]**

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

## **Anlage A – Technische Infrastruktur**

Als Beispiel ist hier die Gliederung der original Anlage wiedergegeben. Die Anlage ist von der Einrichtung anhand der tatsächlich vorliegenden Infrastruktur zu erstellen.

### **A.1. Grundlagen**

#### **A.1.1. Passive Infrastruktur**

##### **A.1.1.1. Primäre Verkabelung**

**Verwendete LWL-Kabel**

**Steckertypen**

**Netztopologie und Dokumentation**

##### **A.1.1.2. Sekundäre Verkabelung**

##### **A.1.1.3. Tertiäre Verkabelung**

#### **A.1.2. Technische Vorgaben**

##### **A.1.3. Auswahl von Standorten für Wiring-Center**

###### **A.1.3.1. Raumbedarf**

###### **A.1.3.2. Ausstattung von Wiring-Centern**

**Stromversorgung**

**Netzschränke**

###### **A.1.3.3. Zugangsregelungen für Wiring-Center**

### **A.2. Aktive Infrastruktur**

#### **A.2.1. Campus-Backbone**

**ATM**

**Gigabit-Ethernet**

**Routing**

**Standortübergreifende Layer 2 VLANs:**

##### **A.2.2. Aktive Komponenten im Bereich der tertiären Vernetzung / Versorgung der Endgeräte**

##### **A.2.3. Weitere Anschlussvarianten an das Campusnetz**

**Richtfunkverbindungen**

**WLAN-Richtfunk**

**ISDN und DSL**

#### **A.3. Anbindung an das Internet**

#### **A.4. Drahtlose Netze (FUNKLAN)**