IT-Sicherheitsrichtlinie für die Goethe-Universität Frankfurt

Version 1.0.12

Steckbrief

Zielsetzung	Einheitliche Sicherheitsstandards zur Gewährleistung eines ordnungsgemäßen IT-Betriebs
Regelungsinhalte	Regelungen zur Informationssicherheit und Datenschutz
Zielgruppe	Alle Mitglieder der Goethe-Universität Frankfurt und Nutzer deren IT-Ressourcen
Geltungsbereich	Alle Einrichtungen der Goethe-Universität Frankfurt
Gültigkeitsdauer	Unbegrenzt

Gliederung

Autoren

Mitglieder des Sicherheitsmanagement-Teams

Hr. E. Schleiff (FB 15, Vizepräsident)

Hr. U. Kebschull (Leiter HRZ)

Fr. Ch.v. Scheven (Datenschutzbeauftragte)

Hr. E. Hillrichs (Leiter Referat Arbeitssicherheit)

Fr. C. Lüdde (HRZ, ehemalige IT-Sicherheitsbeauftragte)

Hr. A. Zeidan (HRZ, IT-Sicherheitsbeauftragter)

Abgestimmt mit der Personalvertretung und den IT-Beauftragten.

Dieses Dokument basiert auf der Sicherheitsrichtlinie der Freien Universität Berlin

Inhaltsverzeichnis

Verzeichnis der IT-Grundschutzmaßnahmen

Präambel

Um das Ziel „ausreichende und angemessene IT-Sicherheit[1]“ in der Goethe-Universität Frankfurt zu erreichen, werden die Empfehlungen und Vorschläge des Bundesamts für Sicherheit in der Informationstechnik (BSI) zugrunde gelegt. Ausgehend von der Annahme, dass Datenschutz und Informationssicherheit einander gleichberechtigt und wechselseitig ergänzen, sind beide Gesichtspunkte integraler Bestandteil dieser Richtlinie. Damit soll ein systematischer Weg beschritten werden, der zu einem ganzheitlichen und vollständigen Ergebnis führt. Voraussetzung dafür ist die konstruktive Zusammenarbeit aller Beteiligten.

Gleichzeitig sollen die Ausführungen in dieser Richtlinie allen Betroffenen eine Handreichung sein, die notwendigen und angemessenen Sicherheitsvorkehrungen bei der Planung und dem Betrieb von Daten verarbeitenden Systemen auszuwählen.

[1] IT = Informationstechnik

1. Geltungsbereich

Die in dieser IT-Sicherheitsrichtlinie beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind für Mitglieder, Angehörige und Einrichtungen der Goethe-Universität Frankfurt gemäß Hochschulgesetz verbindlich. Die IT-Sicherheitsrichtlinie gilt darüber hinaus auch für alle externen Nutzer der IT-Infrastruktur der Goethe-Universität Frankfurt sowie für alle im Universitätsnetz betriebenen IT-Systeme.

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

2. Ausgangssituation

Die Goethe-Universität Frankfurt setzt in hohem Maße Informationstechnologie 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, elektronische Bibliothekssysteme oder das elektronische Management von Lehrveranstaltungen
- Verwaltung: zum Beispiel Verwaltung von Personal-, Studierenden und Prüfungsdaten, Finanzsteuerung

Verbunden mit dem steigenden IT-Einsatz an der Goethe-Universität Frankfurt steigt auch die Abhängigkeit der Universität vom Funktionieren der IT. Der zuverlässige IT-Einsatz ist notwendig auf Grund von

- Gesetzlichen Anforderungen: zum Beispiel Datenschutz, Haushalts-, Steuer-, Urheber- und Strafrecht
- Vertraglichen Anforderungen: zum Beispiel die Nutzung des DFN-Netzes und die Revisionspflicht gegenüber Drittmittelgebern
- Empfehlungen der Verbände der Hochschulen, zum Beispiel Empfehlung der HRK zum Umgang mit wissenschaftlichem Fehlverhalten in den Hochschulen
- Selbstverpflichtung: zum Beispiel die Grundsätze der Goethe-Universität zur Sicherung guter wissenschaftlicher Praxis (wissenschaftliche Primärdaten müssen 10 Jahre aufbewahrt werden)

Es sind daher Maßnahmen zu treffen, die die Funktionsfähigkeit der Goethe-Universität Frankfurt gewährleisten. Die Maßnahmen sollen Schadensereignisse abwehren und so Schäden vermeiden, die durch höhere Gewalt, technisches Versagen, vorsätzliche Handlungen, Nachlässigkeit oder Fahrlässigkeit drohen.

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

Sicherheitsrichtlinie verbindlich beschrieben und entsprechend dem Stand der Technik anzuwenden.

Für das geordnete Zusammenwirken ist eine Verständigung über die verwendete Terminologie erforderlich. Deshalb werden zunächst (siehe Abschnitt 2.1) die in der IT-Sicherheitsrichtlinie der Goethe-Universität Frankfurt enthaltenen zentralen Begriffe erläutert.

Die Beschreibung des Umgangs mit der an der Goethe-Universität Frankfurt eingesetzten Informationstechnologie erfolgt in IT-Verfahren (siehe Abschnitt 2.2) und ist ein wesentlicher Bestandteil des IT-Sicherheitsprozesses. Für die Festlegung des Schutzbedarfs der zu Grunde liegenden Daten ist jeweils eine Schutzbedarfsanalyse (siehe Kapitel 4) durchzuführen.

Der für jeden IT-Arbeitsplatz zu erreichende Minimalschutz bildet das Fundament der IT-Sicherheit der Goethe-Universität Frankfurt. Die zur Erreichung des Minimalschutzes erforderlichen Maßnahmen werden unabhängig von den einzelnen Verfahren beschrieben. Für IT-Verfahren mit höherem Schutzbedarf müssen über diese Schutzmaßnahmen hinaus zusätzliche verfahrensbezogene Maßnahmen erarbeitet werden (s. Abschnitt 4ff.).

Aufgrund des stetigen Fortschritts auf dem Gebiet der Informationstechnik müssen die IT-Sicherheitsrichtlinie und die daraus folgenden Beschlüsse, insbesondere Handlungsanweisungen regelmäßig überprüft und neuen Anforderungen angepasst werden. Die Veröffentlichung der Beschlüsse und Handlungsanweisungen erfolgt auf einer noch bekanntzugebenden Webseite der Goethe-Universität.

Auf die bisher bestehenden Regelungen der Goethe-Universität wird in diesem Zusammenhang hingewiesen:

- IT- Sicherheitsordnung der Goethe-Universität vom 07.Mai 2013 (UniReport 14. Mai 2013)

- Allgemeine Nutzungsordnung für die Informationsverarbeitungs-und Kommunikations-Infrastruktur der Johann Wolfgang Goethe-Universität (Allgemeine IuK-Nutzungsordnung) vom 11.September 2008 (UniReport 23.September 2008)

- Satzung der Johann Wolfgang Goethe-Universität zum Studienausweis als Chipkarte vom 6. September 2006 (Chipkarten-Satzung) in der Fassung vom 11. September 2008 (UniReport 23. September 2008)

- Satzung der Johann Wolfgang Goethe-Universität über die Einführung der Universitätskarte „Goethe-Cardplus“ vom 31. März 2009 -Satzung Goethe-Cardplus (UniReport 03.April 2009)

Weitere Regelungen werden auf der Seite der Universität (http://www.satzung.uni-frankfurt.de) veröffentlicht

2.1 Grundbegriffe der IT-Sicherheitsrichtlinie

Im Folgenden werden die zentralen Begriffe der IT-Sicherheitsrichtlinie der Goethe-Universität Frankfurt erläutert.

- **Geschäftsprozess**
  Ein Geschäftsprozess im Sinne dieser Richtlinie ist eine Abfolge von zusammenhängenden wiederkehrenden IT-gestützten Aktivitäten mit definierten Ein- und Ausgaben.
- **IT-Verfahren**
  Ein IT-Verfahren besteht aus einem Geschäftsprozess oder ist eine Zusammenfassung von mehreren Geschäftsprozessen, die ein gemeinsames Ziel verfolgen.
- **Verfügbarkeit**
  Verfügbarkeit bezieht sich auf Daten und Verfahren und bedeutet, dass sie zeitgerecht zur Verfügung stehen.
- **Vertraulichkeit**
  Vertraulichkeit ist gewährleistet, wenn nur Personen, die dazu berechtigt sind, von schützenswerten Daten Kenntnis nehmen können.
- **Integrität**
  Integrität ist gewährleistet, wenn schützenswerte Daten unversehrt und vollständig bleiben.
- **Transparenz**
  Transparenz ist gewährleistet, wenn das IT-Verfahren für die jeweils Sachkundigen in zumutbarer Zeit mit zumutbarem Aufwand nachvollziehbar ist. Für Betroffene muss die Verarbeitung ihrer Daten vollständig nachvollziehbar sein. In der Regel setzt dies eine aktuelle und angemessene Dokumentation voraus.
- **Authentizität**
  Authentizität bedeutet, dass Daten jederzeit ihrem Ursprung zugeordnet werden können.
- **Revisionsfähigkeit**
  Revisionsfähigkeit bezieht sich auf die Organisation des Verfahrens. Sie ist gewährleistet, wenn Änderungen an Daten nachvollzogen werden können.
- **Datenvermeidung, Datensparsamkeit und Erforderlichkeit**
  Diese Begriffe bedeuten, dass Daten nur in dem Umfang erhoben und verarbeitet werden, wie es für die Erfüllung der Aufgaben mindestens erforderlich sind.
- **Zweckbindung**
  Daten dürfen nur für den Zweck verwendet werden, zu dem sie erhoben wurden.
- **Intervenierbarkeit**
  Intervenierbarkeit ist gegeben wenn ein IT-Verfahren es ermöglicht, in seinen Ablauf steuernd einzugreifen, so dass beispielsweise Rechte von Betroffenen jederzeit gewahrt werden können.
- **Informationelles Selbstbestimmungsrecht**
  Betroffene haben das Recht, selbst über die Preisgabe und Verwendung ihrer Daten zu entscheiden.

2.2 IT-Verfahren und Geschäftsprozesse

Ein IT-Verfahren besteht aus einem oder mehreren IT-gestützten Geschäftsprozessen, die eine arbeitsorganisatorisch abgeschlossene Einheit mit einem gemeinsamen Ziel bilden. Die Summe aller IT-Verfahren soll den gesamten IT-Einsatz in der Goethe-Universität Frankfurt lückenlos abbilden.

2.2.1 Erfassung und Dokumentation von IT-Verfahren

Alle IT-Verfahren müssen dem Sicherheitsmanagement-Team (SMT) über dessen Vorsitz angezeigt werden. Darüber hinaus müssen alle IT-Verfahren in einem für die Goethe-Universität verbindlichen System dokumentiert werden. Inhalt und Umfang einer IT-Verfahrensdokumentation sind abhängig von der Art der im IT-Verfahren erfassten Geschäftsprozesse, der eingesetzten IT-Systeme und der Art der zu verarbeitenden Daten. Zu den unverzichtbaren Bestandteilen der Dokumentation eines IT-Verfahrens gehören:

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

b) Schutzbedarfsanalyse

c) Notfallplan

d) Risikoanalyse in Abhängigkeit vom Ergebnis der Schutzbedarfsanalyse

e) Beschreibung der Rollen; ggf. in Form eines Berechtigungskonzepts

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

g) Angaben der Schnittstellen zu anderen IT-Verfahren, IT-Systemen und sonstigen Diensten

h) Angaben über die vom IT-Verfahren betroffenen Personen und Organisationseinheiten

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

j) Zeitplan für die Einführung des Verfahrens sowie ggf. für die Erstellung eines Betreuungskonzepts

k) Betriebshandbuch mit allen für den Betrieb notwendigen Angaben über die im IT-Verfahren erfassten technischen Systeme

l) Soweit personenbezogene Daten verarbeitet werden: Angaben über den Umgang mit personenbezogenen Daten (Vorabkontrolle gem. § 7 Abs.6 HDSG, Verfahrensverzeichnis gem. § 6 HDSG)

Abweichend von den vorangegangenen Dokumentationskriterien gilt für den Betrieb von IT-Systemen in Forschungsprojekten (außer Infrastruktur) und für IT-Systeme mit kurzer Betriebsdauer (weniger als sechs Monate) in der Regel keine Pflicht zur ausführlichen Verfahrensbeschreibung. Die Anzeige für IT-Verfahren muss dann die beabsichtigte Laufzeit und ggf. den Forschungszusammenhang benennen. Das Sicherheitsmanagement-Team behält sich vor in Zweifelsfällen eine ausführliche Dokumentation zu verlangen.

Auch wenn für IT-Systeme in Forschungsprojekten und für IT-Systeme mit kurzer Betriebsdauer keine Verpflichtung zur Durchführung einer Schutzbedarfsanalyse und ggf. einer Risikoanalyse bestehen, muss dennoch die Sicherheit der eingesetzten betroffenen Systeme sowie der zugrunde liegenden Infrastruktur gewährleistet werden. Unberührt bleibt für IT-Systeme mit kurzer Betriebsdauer im Fall der Verarbeitung von personenbezogenen Daten die Dokumentation gemäß Ziffer l).

Wichtige Merkmale eines IT-Verfahrens sind der längerfristige Charakter der erfassten IT-gestützten Arbeitsabläufe. Ein IT-Verfahren wird üblicherweise über mehrere Jahre hinweg betrieben. Bei der Festlegung von IT-Geschäftsprozessen wie auch von IT-Verfahren soll der Grundsatz der Generalisierung bzw. der Zusammenfassung beachtet werden. Der IT-Geschäftsprozess bildet bei der Erfassung des IT-Einsatzes die kleinste Einheit und ist als eine sequenzielle und/oder parallele Abfolge von zusammenhängenden IT-gestützten und/oder IT-unterstützenden Tätigkeiten definiert. Als Anhaltspunkt für eine Zusammenfassung oder eine Trennung von Arbeitsabläufen können u. a. folgende Kriterien dienen:

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

Tabelle 1: Kriterien für IT-Verfahren.

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

- Beispiel für ein IT-Verfahren mit nur einem Geschäftsprozess: **PC-Pool**
  Der Betrieb eines PC-Pools beinhaltet typischerweise nur einige wenige Tätigkeiten, die alle der Bereitstellung von PCs dienen. Die Aufteilung der Tätigkeiten in verschiedene Geschäftsprozesse ist aufgrund der geringen Komplexität nicht sinnvoll.

- Beispiel für ein IT-Verfahren mit mehreren Geschäftsprozessen: **Campus Management**
  Das Campus-Management-System umfasst eine Vielzahl von zusammenhängenden Prozessen in verschiedenen Organisationseinheiten der Goethe-Universität Frankfurt. Beispielsweise müssen zu Beginn eines Semesters die Anmeldevorgänge der Studierenden zu den Lehrveranstaltungen und am Ende eines Semesters die Prüfungsergebnisse erstellt und verwaltet werden. Beide Prozesse sind relativ komplex und beinhalten eine Reihe von verschiedenen Abläufen in unterschiedlichen Einrichtungen (Studierendensekretariat, Prüfungsämter, Hochschulrechenzentren, usw.) mit verschiedenen Akteuren (Mitarbeiter im Studierendensekretariat und in den Prüfungsämtern, Dozenten, Studierende, usw.).

Allgemein gilt, dass es normalerweise nicht sinnvoll ist, einzelne Tätigkeiten, wie z.B. die Erledigung der Korrespondenz, als einen eigenen Geschäftsprozess oder sogar als ein eigenes IT-Verfahren festzulegen. Dadurch würde eine große Zahl von IT-Geschäftsprozessen bzw. Verfahren entstehen, deren strukturierte Bearbeitung kaum mehr leistbar ist.

Die IT-Verfahrensdokumentation muss stets auf dem aktuellen Stand gehalten werden. Bei wesentlichen Änderungen eines IT-Verfahrens muss zeitnah eine Änderungsmeldung an das Sicherheitsmanagement-Team erfolgen. Damit die Aktualität der Daten gewährleistet ist, sind alle

Einrichtungen der Goethe-Universität Frankfurt verpflichtet, jährlich jeweils zum 1. März die Aktualität der Dokumentation zu melden. Die Meldung erfolgt durch die

- Bestätigung des unveränderten Betriebs oder
- Aktualisierung der Verfahrensbeschreibung (Änderungsmeldung) oder
- Mitteilung über die Einstellung eines IT-Verfahrens.

2.2.2 Rollen für IT-gestützte Geschäftsprozesse

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 Rollenverteilung innerhalb eines IT-Verfahrens / IT-Geschäftsprozesses orientiert sich an folgendem Rollenmodell[2].

Rolle	Funktion	Erforderlichkeit
Verfahrens-verantwortlicher	▪ organisiert die Einführung und den Betrieb eines Dienstes ▪ verantwortlich für die technische Durchführung bzw. die Erstellung eines Dienstes ▪ verantwortlich für die korrekte Umsetzung der Vorgaben ▪ verantwortlich für alle IT-Aufgaben, die im Rahmen des Verfahrens anfallen ▪ verantwortlich für die technische Umsetzung des Datenschutzes und der Informationssicherheit	obligatorisch für jedes IT-Verfahren
Systemadministrator	▪ konfiguriert und betreibt IT-Systeme ▪ zuständig für den ordnungsgemäßen Betrieb der IT-Systeme ▪ evtl. zuständig für die Erstellung eines Betriebs- und Datensicherungskonzepts ▪ zuständig für die Einhaltung eines Betriebs- und Datensicherungskonzepts	grundsätzlich vorhanden
Applikationsbetreuer	▪ Parametrisierung und Konfiguration der Anwendungssoftware ▪ Verwaltung von festgelegten Benutzerrechten ▪ administrative Betreuung aus fachlicher Sicht neben und ergänzend zur Systemadministration	grundsätzlich vorhanden
Anwenderbetreuer	▪ i.d.R. zuständig für die Installation und Wartung von Endgeräten und Anwendungssoftware ▪ erste Ansprechstelle für Anwender (neben dem Key-User)	bei komplexeren Systemen häufig vorhanden
Key-User	▪ Key-User verfügen über besonders gute Anwendungskenntnisse, die sie an die Anwender weitergeben (Multiplikatoren) ▪ erste Ansprechstelle für Anwender (neben dem Anwenderbetreuer)	bei komplexeren Systemen mit vielen Anwendern häufig vorhanden
Anwender	▪ nutzen im Rahmen der ihnen zugewiesenen Berechtigungen die IT-Ressourcen der Goethe-Universität Frankfurt	grundsätzlich vorhanden

Tabelle 2: Übersicht der Rollen.

[2] Die Fachverantwortung ist häufig anders geregelt als die IT-Verantwortung.

Die konkrete personelle Zuordnung einer Rolle ist abhängig von dem betreffenden IT-Verfahren bzw. IT-Geschäftsprozess. Zum Beispiel kann bei großen und komplexen IT-Geschäftsprozessen die Rolle des Applikationsbetreuers auf mehrere Personen verteilt sein. Anderseits kann bei kleinen IT-Geschäftsprozessen diese Rolle von einer Person übernommen werden, die gleichzeitig auch die Rolle eines Anwenderbetreuers und/oder Key-Users ausfüllt. Eine Rolle kann also von einer oder mehreren Personen ausgefüllt werden. Darüber hinaus ist zu beachten, dass nicht alle dargestellten Rollen in einem konkreten IT-Geschäftsprozess zwingend notwendig sind. Die Rolle des Verfahrensverantwortlichen ist aber für jedes IT-Verfahren zwingend notwendig und muss von einer einzigen natürlichen Person wahrgenommen werden.

Das Zusammenwirken der verschiedenen Rollen soll in der folgenden Grafik veranschaulicht werden.

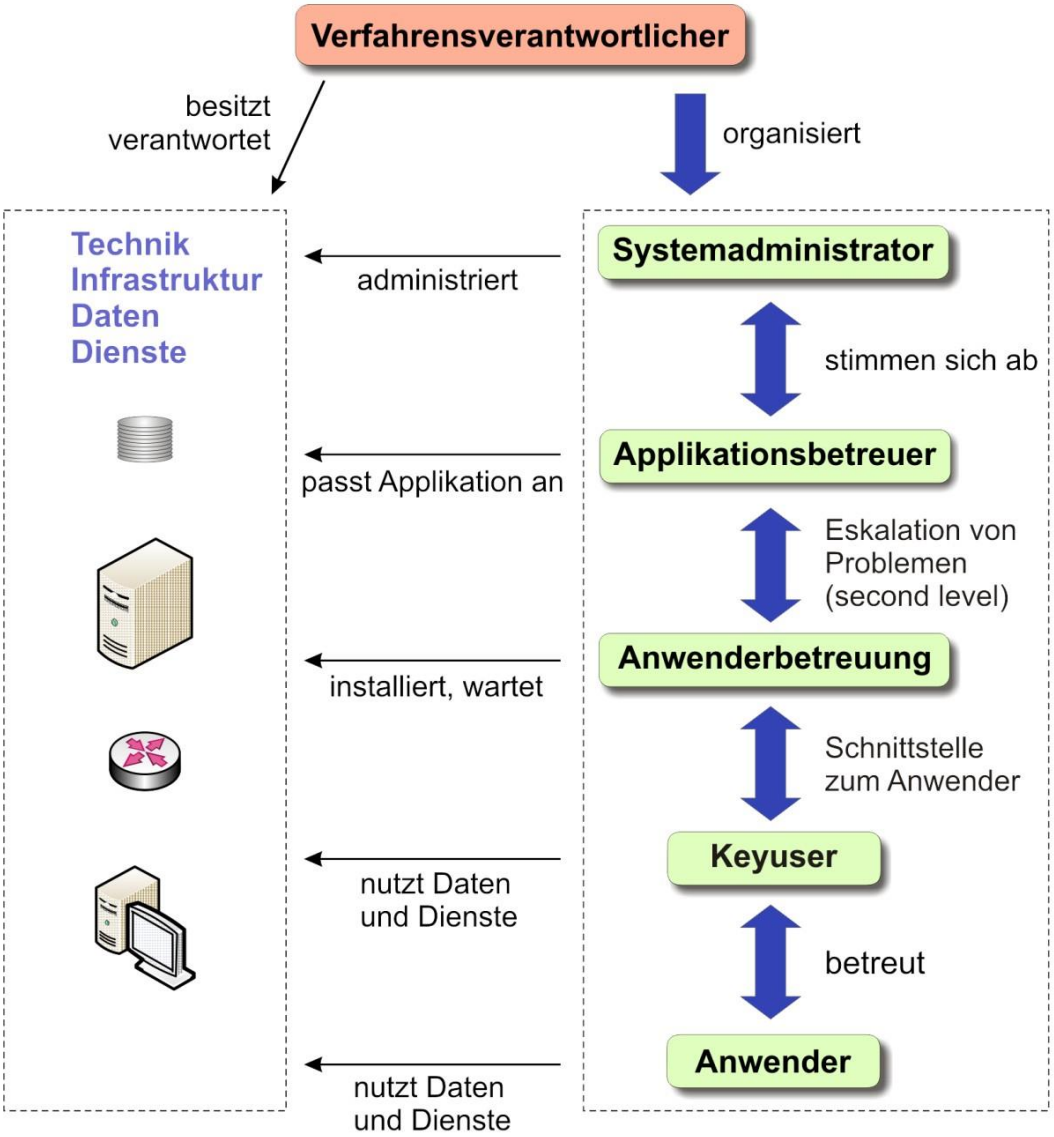

Abbildung 1: Zusammenwirken der Rollen.

2.3 Verantwortlichkeiten und Organisation der IT-Sicherheit

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

Die an der Universität für den IT-Einsatz aus organisatorischer und strategischer Sicht bedeutendsten Rollen insbesondere auf Grundlage der IT- Sicherheitsordnung der Goethe-Universität vom 07.Mai 2013 (IT-SO) sollen an dieser Stelle kurz dargestellt werden:

- **Höchste Entscheidungsinstanz (Präsidium)**
  Die höchste Entscheidungsinstanz an der Goethe-Universität Frankfurt in allen IT-Fragen ist das Präsidium bzw. der Präsident der Goethe-Universität Frankfurt. Es ist für alle Aufgaben der strategischen Führung der Informationstechnologie und der bereichsübergreifenden operativen Vorgaben verantwortlich.

- **Koordination und Organisation der Informationssicherheit (IT-Sicherheitsbeauftragte(r)) gemäß §§ 4 Abs.1, 6 Abs.2 in Verb. m.§ 7 IT-SO**
  Die Rolle der/des IT-Sicherheitsbeauftragten obliegt dem für IT zuständigen Vizepräsidenten oder eine vom Präsidium beauftragte Person. Sie/er hat die Aufgabe der Koordination und Organisation der Informationssicherheit. Er ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Goethe-Universität Frankfurt. Zu den Aufgaben des IT-Sicherheitsbeauftragten gehören u.a.:
  - Den Sicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
  - die Erstellung der IT-Sicherheitsrichtlinie und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren.

- **IT-Sicherheits-Management-Team (SMT) gemäß §§ 5, 6 IT-SO**
  Zu den zentralen Aufgaben des SMT gehören insbesondere:
  - IT-Sicherheitsziele und -strategien zu bestimmen sowie die IT-Sicherheitsrichtlinie zu entwickeln,
  - Beschlussfassungen, insbesondere Erlass von Handlungsanweisungen zur IT-Sicherheit und IT-Funktionsfähigkeit,
  - den IT-Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
  - zu überprüfen, ob die in der IT-Sicherheitsrichtlinie geplanten IT-Sicherheitsmaßnahmen wie beabsichtigt funktionieren also geeignet und wirksam sind,
  - bei der Fortschreibung der IT-Sicherheitsrichtlinie mitzuwirken,
  - die Schulungs- und Sensibilisierungsprogramme für IT-Sicherheit zu konzipieren sowie
  - die Leitungsebene in IT-Sicherheitsfragen zu informieren und zu beraten.

  Die Zusammensetzung des SMT soll möglichst die Vielfalt der unterschiedlichen Anforderungen der Organisationseinheiten (Forschung und Lehre, Dienstleister, Verwaltung)

an den IT-Einsatz berücksichtigen.

- **Datenschutz (Behördlicher Datenschutzbeauftragter) gemäß § 5 HDSG**
  Die Unterstützung der Universitätsleitung in allen Fragen der Verarbeitung personenbezogener Daten und die Überwachung der ordnungsgemäßen Anwendung Datenverarbeitender Programme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, obliegen dem behördlichen Datenschutzbeauftragten. Er fungiert als Ansprechpartner für die Angehörigen der Goethe-Universität Frankfurt und macht die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Erfordernissen des Datenschutzes vertraut.

- **Bereitstellung von zentralen und überregionalen IT-Diensten (Zentrale IT-Dienstleister)**
  Die zentralen IT-Dienstleister (insbesondere Hochschulrechenzentrum (HRZ), Universitätsbibliotheks-IT, HeBIS-IT, Business Application Management (BAM)) planen, realisieren, betreiben und gestalten IT-Infrastrukturen und -Services für die Fachbereiche und Einrichtungen der Goethe-Universität Frankfurt.

- **Bereichsbezogener IT-Einsatz (Bereichsleitung)**
  Die Leitung einer Organisationseinheit trägt die Verantwortung für den laufenden IT-Einsatz in ihrem Aufgabenbereich sowie für alle bereichsinternen IT-Planungen. Gemeinsam mit dem Verfahrensverantwortlichen gibt die Bereichsleitung auf der Grundlage der Ergebnisse der Schutzbedarfs- und ggf. Risikoanalyse den Betrieb des IT-Verfahrens frei. Sie benennt einen IT-Beauftragten, der den IT-Einsatz koordiniert und plant und darüber hinaus die in der IT-Sicherheitsrichtlinie formulierten Maßnahmen umsetzt.

- **Bereichsbezogener IT-Einsatz (IT-Beauftragter) gemäß §§ 4 Abs.2, 6 Abs.3 IT-SO**
  Zu den zentralen Aufgaben eines IT-Beauftragten gehören:
  - Ansprechpartner für Mitarbeiter der betreffenden Organisationseinheit in Fragen der IT-Organisation und IT-Sicherheit
  - Ansprechpartner der betreffenden Einrichtung für alle Gremien und andere Organisationseinheiten in allen IT-Fragen
  - Erfassung und Dokumentation des bereichsinternen IT-Einsatzes
  - Koordination und Kontrolle der IT-Beschaffung
  - Überwachung der Umsetzung von zentralen Vorgaben zum IT-Einsatz
  - Mitarbeit bei der bereichsinternen Planung bei allen Fragestellungen mit IT-Relevanz
  - Mitarbeit bei der Erstellung und Umsetzung von bereichsübergreifenden IT-Konzepten
  - die Realisierung für IT-Sicherheitsmaßnahmen zu initiieren und zu prüfen
  - der Leitungsebene und dem Sicherheitsmanagement-Team über den Status Quo der IT-Sicherheit zu berichten
  - Koordination von sicherheitsrelevanten Projekten
  - Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahme

- **Verantwortung für den Betrieb eines IT-Verfahrens (Verfahrensverantwortlicher)** Der Verfahrensverantwortliche organisiert die Einführung und den laufenden Betrieb eines IT-Verfahrens einschließlich aller Komponenten und Schnittstellen. Er ist für die Durchführung einer Fachaufgabe bzw. die Erstellung eines Dienstes verantwortlich und in der Regel „Besitzer“ der verarbeiteten Daten. Insbesondere trägt er auch die Verantwortung für die Einhaltung des Datenschutzes und der Informationssicherheit. (Siehe auch Abschnitt 2.2.2).

3. IT-Grundschutz

Sicherheit und Datenschutz in der Informationstechnik dienen der Sicherstellung von Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Revisionsfähigkeit von Daten und IT-Anwendungen. Bei der Verarbeitung personenbezogener Daten sind darüber hinaus die Prinzipien der Datenvermeidung, Datensparsamkeit und Erforderlichkeit sowie der Zweckbindung, Intervenierbarkeit und ggf. Handlungsanweisungen des SMT zu beachten. Sie sind nur durch ein Bündel von Maßnahmen aus den Bereichen Organisation, Personal, Infrastruktur, Hard- und Software, Kommunikation und Notfallvorsorge zu erreichen.

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

3.1 Definition des Grundschutzes

Die Schutzwürdigkeit von Daten und Verfahren ist nicht einheitlich. Daher unterscheiden sich auch die jeweils angemessenen Schutzmaßnahmen. Die hier für den Grundschutz zusammengestellten Maßnahmen gewährleisten ausreichende Sicherheit bei vielen IT-Verfahren. Sie bilden die Grundlage für alle IT-Verfahren bzw. Geschäftsprozesse der Goethe-Universität Frankfurt. Ihre Realisierung in den Organisationseinheiten ist insbesondere notwendige, aber nicht immer hinreichende Voraussetzung für die Teilnahme an übergreifenden IT-Verfahren wie der Nutzung zentraler Dienste, zum Beispiel E-Mail, Benutzung des Datennetzes oder dem Identitätsmanagement der Goethe-Universität Frankfurt.

Für viele IT-Verfahren mit einem Schutzbedarf „normal“ ist die Umsetzung der Grundschutzmaßnahmen zum Erreichen eines angemessenen Sicherheitsniveaus ausreichend. Für IT-Verfahren mit hohem und sehr hohem Schutzbedarf müssen über diese Grundschutzmaßnahmen hinaus zusätzliche Maßnahmen umgesetzt werden. Sie sind verfahrensbezogen und aus entsprechenden Risikoanalysen abgeleitet. In einigen in dieser Richtlinie genannten Maßnahmen werden über die Erfordernisse des Grundschutzes hinausreichende Handlungsempfehlungen gegeben. Bei jeder Maßnahme ist beschrieben, wer sie initiiert und wer sie verantwortlich umsetzt. Der Maßnahmenkatalog ist allen Anwendern an der Goethe-Universität Frankfurt in geeigneter Weise bekannt zu geben.

Als Basis für die hier dargestellten IT-Grundschutzmaßnahmen dienen die IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die dort beschriebenen Maßnahmen wurden den Besonderheiten der Goethe-Universität Frankfurt angepasst. Die Grundschutzkataloge des BSI beinhalten über 1.200 Maßnahmen und beziehen sich oft sehr detailliert auf einzelne Hard- und Software. Im Unterschied dazu beispielsweise beziehen sich die IT-Grundschutzmaßnahmen der Universität auf ganze Klassen von Programmen. Das bedeutet, dass viele der in dieser Richtlinie dargestellten Maßnahmen allgemeiner gefasst sind.

Die für die Universität geltenden Maßnahmen sollen also nicht in Konkurrenz zu den Maßnahmen des BSI stehen. Stattdessen sollen die BSI-Maßnahmen eine Ergänzung darstellen, wenn beispielsweise detailliertere Betrachtungen einzelner IT-Komponenten notwendig sind. Auf die Behandlung einiger Sicherheitsmaßnahmen zu speziellen Themen wird bewusst verzichtet (z. B. physische Absicherung von Maschinensälen und zentraler Netzwerkinfrastruktur).

Mit dem Begriff „IT-Personal“ werden im Folgenden alle Personen verstanden, die mit der Administration, Wartung und Betreuung von IT-Ressourcen der Goethe-Universität Frankfurt betraut sind, unabhängig von ihrem Beschäftigungs- oder Zugehörigkeitsstatus.

3.2 Maßnahmen des IT-Grundschutzes

3.2.1 Allgemeines

- **Grundsätze für den IT-Einsatz (M1)**

Verantwortlich für Initiierung:	Präsidium
Verantwortlich für Umsetzung:	Bereichsleitung, IT-Beauftragter

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

- **Gesamtverantwortung (M2)**

Verantwortlich für Initiierung:	Präsidium
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 Hessischen Hochschulgesetzes.

3.2.2 Organisation von IT

- **Beschreibung von IT-Verfahren (M3)**

Verantwortlich für Initiierung:	IT-Beauftragter, IT-Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	Verfahrensverantwortlicher

Der gesamte IT-Einsatz ist in IT-Verfahren zu gruppieren. Jedes Verfahren ist zu beschreiben. Die Anforderungen an eine Beschreibung sind in dem Abschnitt 2.2.1 Erfassung und Dokumentation von IT-Verfahren dieser Richtlinie festgelegt.

- **Rollentrennung (M4)**

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

Für jedes IT-Verfahren bzw. jeden IT-Arbeitsprozess sind die Verantwortlichkeiten für alle Bereiche eindeutig festzulegen. Jedem Mitarbeiter müssen die ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein. Abgrenzungen und Schnittflächen der verschiedenen Anwenderrollen müssen klar definiert sein. Bei der Rollenbesetzung muss beachtet werden, dass im Falle von Interessenkonflikten bestimmte Rollen von verschiedenen Personen wahrgenommen werden müssen. Beispielsweise darf im Campus-Management-System die Eintragung von Prüfungsergebnissen nicht von betroffenen studentischen Mitarbeitern durchgeführt werden.

- **Benennung eines IT-Beauftragten (M5)**

Verantwortlich für Initiierung:	Präsidium
Verantwortlich für Umsetzung:	Bereichsleitung

Den IT-Beauftragten der Organisationseinheiten kommt im Rahmen des IT-Einsatzes an der Universität eine zentrale Bedeutung zu, denn sie haben in ihrem Zuständigkeitsbereich die für den IT-Einsatz gebotenen technischen und organisatorischen Maßnahmen zur IT-Sicherheit und Datenschutz zu initiieren und zu koordinieren; sie führen die notwendigen Aufzeichnungen für die Organisationseinheit ihrer Zuständigkeit. Bei Fragen des IT-Einsatzes sind sie sowohl Ansprechpartner für die Mitarbeiter ihrer Organisationseinheit als auch für Dritte (außerhalb ihrer Organisationseinheit). (Siehe Abschnitt 2.3 Verantwortlichkeiten und Organisation der IT-Sicherheit)

- **Einbindung des IT-Beauftragten in Entscheidungsprozesse (M6)**

Verantwortlich für Initiierung:	Präsidium, Bereichsleitung
Verantwortlich für Umsetzung:	Fach-/Bereichsleitung

Damit der IT-Beauftragte seine Aufgaben effizient wahrnehmen kann, sollte die Stelle des IT-Beauftragten organisatorisch der Bereichsleitung direkt unterstellt sein. Er ist in alle Entscheidungsprozesse mit IT-Relevanz einzubeziehen. Insbesondere muss der IT-Beauftragte bei allen IT-Beschaffungsmaßnahmen, bei baulichen Maßnahmen und Umzügen sowie bei den IT-bezogenen Phasen eines Berufungsverfahrens beteiligt werden. Darüber hinaus muss die Fach-/Bereichsleitung sicherstellen, dass der IT-Beauftragte über alle IT-relevanten Vorhaben und Planungen des Bereichs frühzeitig Kenntnis erhält.

- **Dokumentation der IT-Verfahren bezüglich der IT-Sicherheit (M7)**

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

IT-Verfahren sind bezüglich der Sicherheit und des Datenschutzes gemäß den in Abschnitt 2.2.1 formulierten Anforderungen zu dokumentieren.

Nur dokumentierte Verfahren dürfen betrieben werden. Der IT-Beauftragte sorgt für die aktuelle Dokumentation der Verfahren seiner Organisationseinheit. Der IT-Beauftragte ist verantwortlich für die Erstellung und Pflege der Dokumentation der Verfahren seiner Organisationseinheit. Verfahrensverantwortliche, Systemadministratoren und

Applikationsbetreuer sind dabei zur Mitarbeit verpflichtet.

Um seiner Dokumentationspflicht nachkommen zu können, muss sich der IT-Beauftragte auf die Zuarbeit aller betroffenen Mitarbeiter verlassen können. Deshalb ist die Bereichsleitung dafür verantwortlich, dass die notwendige Unterstützung durch die Mitarbeiter gewährleistet ist.

- **Dokumentation von Ereignissen und Sicherheitsvorfällen (M8)**

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

Ereignisse, die Indiz für ein Sicherheitsproblem sein können, sind dem Betreiber des betroffenen Systems zu melden.

Wenn dem Betreiber eines Systems ein Sicherheitsproblem vom Hochschulrechenzentrum oder dem SMT gemeldet wird, ist er verpflichtet, der meldenden Stelle nach Analyse und Beseitigung des Problems eine Freimeldung zu erteilen.

Bei einem Sicherheitsvorfall muss die zuständige IT-Abteilung, das Hochschulrechenzentrum und das SMT informiert werden. Als Sicherheitsvorfall wird ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit oder Integrität der Informationen, Geschäftsprozesse, IT-Dienste und -Anwendungen der Goethe-Universität Frankfurt mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für die Goethe-Universität Frankfurt oder deren Partner entstehen kann. Alle Sicherheitsvorfälle müssen von der zuständigen Stelle dokumentiert werden.

Zuständig für die Dokumentation von Fehlern sind in der Regel der zuständige IT-Bereich einer Einrichtung, die mit IT-Sicherheitsfragen betrauten Stellen oder die Rollenträger, in deren Aufgabengebiet das Ereignis eingetreten ist.

- **Regelungen der Datenverarbeitung im Auftrag (M9)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	Verfahrensverantwortlicher

Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag der Goethe-Universität Frankfurt 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, zum Beispiel bei Umfragen, sind die entsprechenden Regelungen des Hessischen Datenschutzgesetzes zu beachten, insbesondere ist die Zustimmung der Datenschutzbeauftragten der Goethe-Universität einzuholen. Für Wartungsarbeiten, einschließlich Fernwartung, stellt das Hessische Datenschutzgesetz besondere Regelungen bereit, die anzuwenden sind.

- **Standardisierung der technischen Ausstattung (M10)**

Verantwortlich für Initiierung:	Präsidium
Verantwortlich für Umsetzung:	Zentrale IT-Dienstleister, Fachbereiche

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

- **Zentralisierung wichtiger Serviceleistungen (M11)**

Verantwortlich für Initiierung:	Präsidium , Bereichsleitung
Verantwortlich für Umsetzung:	Zentrale IT-Dienstleister, IT-Beauftragter, IT-Personal

Grundsätzlich sind Services, die von IT-Dienstleistungszentren der Goethe-Universität Frankfurt (insbesondere HRZ, Bibliotheks-IT, HeBIS-IT und BAM) bereitgestellt werden, dezentral betriebenen Diensten vorzuziehen. Daher wird eine Reihe von Diensten zentral für die gesamte Goethe-Universität Frankfurt betrieben und angeboten. Dienste müssen zentral betrieben, angeboten und bei Bedarf genutzt werden, wenn die Zentralisierung deutliche Vorteile mit sich bringt (Kosten, räumliche Sicherheit, Notstromversorgung, Klimatisierung etc.).

Nur wenn der benötigte Dienst nicht von zentralen Einrichtungen der Universität bereitgestellt werden kann, dürfen der Dienst und die notwendigen IT-Systeme selbst eingerichtet und betrieben werden

An den spezifischen Bedürfnissen eines Fachbereichs ausgerichtete Dienste, deren Betrieb spezielles wissenschaftliches Know-how erfordert, eignen sich hingegen nicht zur Zentralisierung. Dazu gehören beispielsweise IT-gestützte Messanlagen oder spezielle Auswertungs- und Analyse-Informationstechnik.

In einigen Fällen ist eine Kombination aus zentral und dezentral betriebenen Diensten die beste Lösung. Darunter kann zum Beispiel die vom Hochschulrechenzentrum koordinierte Zusammenarbeit von hochschulrechenzentrumseigenen Services und dezentral betriebenen Services fallen. Beispiele hierfür wären ein virtueller Hochleistungsrechner durch Zusammenwirken mehrerer Computer oder ein virtueller Großspeicher durch Zusammenschalten mehrerer Speicherkapazitäten.

- **Erreichbarkeit von IT-Diensten im Netz (M12)**

Verantwortlich für Initiierung:	Präsidium
Verantwortlich für Umsetzung:	IT-Dienstleister, IT-Personal, Verfahrensverantwortlicher

Die Administration der Sprach- und Datenkommunikationsnetze wird durch das HRZ durchgeführt.

Grundsätzlich ist für das gesamte Campusnetz ein Basisschutz eingerichtet. Für Bereiche mit höherem Schutzbedarf besteht die Möglichkeit, Instanzen einer zentralen Firewall zu nutzen, die von jedem Bereich selbst administriert werden muss. Der Betrieb des Firewallsystems findet im HRZ statt.

Für Einrichtungen der Goethe-Universität Frankfurt, deren Forschungsgegenstand die Netzinfrastruktur oder netzbasierte Dienste ist, kann der IT-Beauftragte der Einrichtung direkt mit den dafür zuständigen Stellen des HRZ Ausnahmeregelungen vereinbaren.

- **Revision der Sicherheit (M13)**

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

Die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit und des Datenschutzes sind regelmäßig und nach jeder Änderung der Sicherheitsstandards zu überprüfen. Zeitgleich mit der Änderung der Maßnahmen muss die Dokumentation aktualisiert werden. Bei der Vergabe der Prüfaufgaben an externe Auftragnehmer ist auf deren Seriosität besonderen Wert zu legen.

- **Allgemeine Notfallvorsorge (M14)**

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

Bei IT-Verfahren bzw. IT-Arbeitsprozesse werden im Rahmen der Dokumentationspflichten Analysen zur Ermittlung des Schutzbedarfs und ggf. zur Identifizierung und Begegnung spezifischer Risiken vorgenommen. Basierend auf den Ergebnissen dieser Analysen sollte ein Notfallplan erstellt werden, in dem festgelegt wird, wie auf Notfallsituationen adäquat reagiert wird. „Notfall“ bezeichnet eine Situation, in der durch eine Betriebsstörung die Sicherheit der IT und der Schutz der Daten nicht mehr gegeben ist und ein verhältnismäßig hoher Schaden entstehen kann. In einem Notfallplan sollten zum Beispiel Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten und zum Einsatz von Ausweichmöglichkeiten enthalten sein. Mindestens sollte ein Alarmierungsplan erstellt werden, in dem die Meldewege und die Kontaktdaten der beteiligten Stellen und Personen im Notfall beschrieben sind. Im Interesse einer möglichst guten Erreichbarkeit ist es bei der Dokumentation der Kontaktdaten häufig sinnvoll, sogenannte Funktions-E-Mail-Adressen oder Sammel-Telefonnummern zu nutzen.

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

3.2.3 Personal

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 (M15)**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	Bereichsleitung

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

- **Angemessene Personalausstattung (M16)**

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

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

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

- **Vertretung (M17)**

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

Für alle Betreuungs- und Administrationsfunktionen sind Vertretungsregelungen erforderlich. Die Vertreter müssen alle notwendigen Tätigkeiten ausreichend beherrschen und ggf. auf schriftliche Arbeitsanweisungen und Dokumentationen zurückgreifen können. Die Vertretungsregelung muss organisatorisch und nach Möglichkeit auch technisch festgelegt sein. Die technischen Voraussetzungen für die Wahrnehmung einer Vertretung sollten möglichst ständig eingerichtet sein.

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

- **Qualifizierung (M18)**

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

IT-Personal soll 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 das IT-Personal in seinen Aufgabengebieten regelmäßig weitergebildet wird.

3.2.4 Sicherung der Infrastruktur

- **Zugang zu Räumen mit zentraler Netzinfrastruktur (M19)**

Verantwortlich für Initiierung:	Präsidium, Bereichsleitung
Verantwortlich für Umsetzung:	Für Technik zuständige Abteilung, Bereichsleitung, IT-Beauftragter

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

- **Sicherung der Serverräume (M20)**

Verantwortlich für Initiierung:	IT-Beauftragter, Bereichsleitung
Verantwortlich für Umsetzung:	Für Technik zuständige Abteilung, Bereichsleitung

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

Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; verwendete Schlüssel müssen kopiergeschützt sein. Für die Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen. Der Zutritt muss auf diejenigen Personen begrenzt werden, deren Arbeitsaufgaben dieses erfordern. Das Betreten der Räume darf nur nach vorheriger Anmeldung bei der für die Räume verantwortlichen Stelle erfolgen. Fremdpersonal soll die Serverräume nach Möglichkeit nur unter Aufsicht betreten.

- **Geschützte Aufstellung von Endgeräten (M21)**

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

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

- **Sicherung der Netzknoten (M22)**

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

Zentrale Vernetzungsinfrastruktur ist grundsätzlich in verschlossenen Räumen oder in nicht öffentlich zugänglichen Bereichen in verschlossenen Schränken einzurichten, die

gegen unbefugten Zutritt und Zerstörung ausreichend gesichert sind. Es gelten die gleichen Empfehlungen wie unter M20.

- **Verkabelung und Funknetze (M23)**

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

Die Verkabelung des LAN ist klar zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Netzwerkadministratoren müssen einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung zentraler Komponenten haben. Nicht benutzte Anschlüsse sollten abgeklemmt oder deaktiviert werden. Erweiterungen und Veränderungen an der Gebäudeverkabelung sind mit dem IT-Beauftragten der eigenen Organisationseinheit und mit dem Hochschulrechenzentrum abzustimmen. Funknetze dürfen nur vom Hochschulrechenzentrum betrieben werden.

- **Geschützte Kabelverlegung (M24)**

Verantwortlich für Initiierung:	Bereichsleitung, IT-Beauftragter
Verantwortlich für Umsetzung:	IT-Dienstleister, Für Technik zuständige Abteilung

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

- **Einweisung und Beaufsichtigung von Fremdpersonal (M25)**

Verantwortlich für Initiierung:	IT-Beauftragter
Verantwortlich für Umsetzung:	Bereichsleitung, IT-Personal, Für Technik zuständige Abteilung

Fremde Personen, die in gesicherten Räumen mit IT (z. B. Serverräume) Arbeiten auszuführen haben, müssen beaufsichtigt werden. Personen, die nicht unmittelbar zum IT-Bereich zu zählen sind, aber Zugang zu gesicherten IT-Räumen benötigen, müssen über die Notwendigkeit besonderer Vorsicht beim Arbeiten in gesicherten Räumen belehrt werden. Beispielsweise müssen sie darauf hingewiesen werden, dass Stecker nicht einfach aus Steckdosen herausgezogen werden dürfen.

Alle Aktionen, die von externen Firmen durchgeführt werden, sollen protokolliert werden. Es sei noch einmal auf die Maßnahme M9 verwiesen.

- **Stromversorgung und Überspannungsschutz (M26)**

Verantwortlich für Initiierung:	IT-Beauftragter, Für Technik zuständige Abteilung, Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Dienstleister, IT-Personal, Für Technik zuständige Abteilung

Alle wichtigen IT-Systeme dürfen nur an eine ausreichend dimensionierte und gegen Überspannungen abgesicherte Stromversorgung angeschlossen werden. Eine entsprechende Versorgung ist in Zusammenarbeit mit der Technischen Abteilung herzustellen. Bei dem Einsatz von Geräten mit redundant ausgelegter Stromversorgung sollte darauf geachtet werden, dass die einzelnen Netzteile über getrennt abgesicherte Stromkreise versorgt werden. Die für den Betrieb von IT notwendigen Unterlagen und Informationen zur elektrischen Versorgung sind dem IT-Beauftragten auf Anfrage von den

IT-Dienstleistern bzw. der Technischen Abteilung zur Verfügung zu stellen. Alle Arbeiten an der Stromversorgung müssen mit dem IT-Beauftragten abgestimmt werden.

- **Stromversorgung (M27)**

Verantwortlich für Initiierung:	IT-Beauftragter (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	IT-Dienstleister, IT-Personal, Für Technik zuständige Abteilung

Alle IT-Systeme, die wichtige oder unverzichtbare Beiträge zur Aufrechterhaltung eines geordneten Betriebes leisten, sind mit unterbrechungsfreier Stromversorgung zur Überbrückung von Spannungsschwankungen und Stromunterbrechungen zu versorgen.

- **Brandschutz (M28)**

Verantwortlich für Initiierung:	IT-Beauftragter (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Für Technik zuständige Abteilung, Arbeitssicherheitsbeauftragter

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

- **Schutz vor Wasserschäden (M29)**

Verantwortlich für Initiierung:	IT-Beauftragter (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Für Technik zuständige Abteilung, Arbeitssicherheitsbeauftragter

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

- **Klimatisierung (M30)**

Verantwortlich für Initiierung:	IT-Beauftragter, Bereichsleitung (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Für Technik zuständige Abteilung

Der Einbau von Klimatisierungsanlagen wird erforderlich, wenn der Luft- und Wärmeaustausch von Server- und Rechnerräumen unzureichend ist bzw. hohe Anforderungen an die Be- und Entfeuchtung eines Raums und an die Schwebstoffbelastung gestellt

werden. Die Gewährleistung der zulässigen IT-Betriebstemperatur und demzufolge die Sicherstellung des IT-Betriebs steht in engem Zusammenhang mit dem reibungslosen Einsatz von Klimatisierungsgeräten. Daher müssen die Geräte mit einer hohen Verfügbarkeit und mit genügend Reserveleistungen ausgestattet sein.

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

3.2.5 Hard- und Softwareeinsatz

- **Beschaffung (M31)**

Verantwortlich für Initiierung:	IT-Verfahrensverantwortliche
Verantwortlich für Umsetzung:	IT-Beauftragter

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

- **Softwareentwicklung (M32)**

Verantwortlich für Initiierung:	IT-Verfahrensverantwortliche
Verantwortlich für Umsetzung:	IT-Beauftragter

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

- **Separate Entwicklungsumgebung (M33)**

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

Damit der laufende Betrieb durch die Softwareentwicklung nicht gestört wird, müssen die Entwicklungsarbeiten einschließlich aller Tests in gesicherten Umgebungen stattfinden. Die strikte Trennung von Entwicklung und Produktion gilt insbesondere auch für die Verarbeitung von schützenswerten Daten. Die Überführung der Software von der Entwicklung in den Produktionsbetrieb bedarf der Freigabe durch den zuständigen IT-Beauftragten oder explizit dafür benannte Personen.

- **Entwicklung von Software nach standardisierten Verfahren (M34)**

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

Die Entwicklung großer, komplexer Systeme muss nach den Regeln anerkannter Vorgehensmodelle zur Softwareentwicklung durchgeführt werden. Beispiel: "Planung und Durchführung von IT-Vorhaben in der Bundesverwaltung" (V-Modell).

- **Kontrollierter Softwareeinsatz (M35)**

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

Auf Rechnersystemen, die IT-Ressourcen der Goethe-Universität Frankfurt nutzen, 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 ist nur gestattet, wenn eine Genehmigung der zuständigen Stelle vorliegt oder eine Organisationseinheit eine pauschale Freigabe für Teilbereiche festgelegt hat.

- **Test von Software auf Servern (M36)**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
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.

- **Sicherheit von Betriebssystemen und Anwendungen (M37)**

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

Sicherheitsrelevante Updates und Patches müssen, soweit möglich, zeitnah eingepflegt werden. Ausnahmen müssen dokumentiert werden.

- **Schutz vor Schadprogrammen (M38)**

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

Auf allen IT-Systemen ist ein Schutz gegen Schadsoftware nach dem aktuellen Stand der Technik einzurichten. Das HRZ bietet ein Virenschutzsystem an. Regelmäßig (möglichst automatisiert) sind die Virenerkennungsmuster zu aktualisieren. Wird auf einem System schädlicher Programmcode entdeckt, muss die zuständige Stelle immer dann informiert werden, wenn die Schadsoftware nicht zuverlässig entfernt werden kann.

Empfehlenswert ist, bei konkretem Bedarf oder Verdacht eine Suche nach Schadprogrammen auf allen bedrohten IT-Systemen vorzunehmen.

- **Schutz der Geräte-Konfiguration von IT-Systemen (M39)**

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

Die Konfiguration von IT-Systemen muss durch angemessene und geeignete Maßnahmen geschützt werden. Der Umfang der Schutzmaßnahmen richtet sich nach der Bedeutung des Rechners für den laufenden Betrieb und nach dem Schutzbedarf der dort verarbeiteten Daten. Z. B. ist bei Arbeitsplatz-Rechnern der Zugriff auf das Rechner-BIOS durch ein Passwort zu schützen.

- **Dokumentation der Hard- und Software (M40)**

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

Die eingesetzten IT-Systeme (Hard- und Software) müssen dokumentarisch erfasst werden. Üblicherweise reichen dafür die von Software-Verteilungs- oder Managementsystemen bereitgestellten Dokumentationswerkzeuge aus. Lediglich spezielle IT-Systeme mit besonderer Bedeutung, wie beispielsweise Hochleistungsrechner oder große Archivsysteme, müssen gesondert dokumentiert werden. Siehe dazu auch Abschnitt 2.2.1 Erfassung und Dokumentation von IT-Verfahren.

- **Ausfallsicherheit (M41)**

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

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

- **Einsatz von Diebstahl-Sicherungen (M42)**

Verantwortlich für Initiierung:	IT-Beauftragter (bereichsspezifisch) Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Für Technik zuständige 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.

- **Datenablage in der Cloud (M43)**

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

Die Speicherung von Daten in öffentlichen Clouds ist zu vermeiden. Wenn Daten mit Hilfe von Cloud-Diensten gespeichert bzw. verarbeitet werden, drohen spezielle Gefahren, die sich insbesondere aus der Überlassung der Daten an externe Dienstanbieter und der dynamischen Verteilung der Speicherkapazitäten über verschiedene Standorte ergeben. Die Eignung oder Nicht-Eignung zur Speicherung in der Cloud richtet sich nach dem Schutzbedarf der Daten. Schützenswerte Daten dürfen dort nur in verschlüsselter Form gespeichert werden. Hoch schützenswerte Daten sind i.d.R. für eine Ablage in der Cloud ungeeignet. Für personenbezogene Daten gelten die Regelungen zur Auftragsdatenverarbeitung des Hessischen Datenschutzgesetzes (Datenverarbeitung innerhalb der EU) bzw. der Betroffene muss der Datenverarbeitung zustimmen (Datenverarbeitung außerhalb der EU).

3.2.6 Einsatz von mobilen Geräten

Durch den zunehmenden Einsatz mobiler Geräte (Smartphones, Notebooks usw.) ergeben sich einerseits spezielle Gefährdungen, wie zum Beispiel ein erhöhtes Diebstahlrisiko. Andererseits sind nicht alle Schutzmaßnahmen geeignet, die für stationäre Systeme anwendbar sind. Die Maßnahmen dieses Abschnitts gehen auf diese spezifischen Gegebenheiten ein.

Bei der Beschreibung und Umsetzung der Maßnahmen spielen die Besitzverhältnisse keine Rolle. Es ist also unerheblich, ob es sich um ein privates oder dienstliches Gerät handelt. Grundlage für die Anwendbarkeit bzw. für den Geltungsbereich der Maßnahmen ist die Inanspruchnahme von Ressourcen (Infrastruktur, IT, Daten usw.) der Goethe-Universität Frankfurt bei der Nutzung des mobilen Geräts.

- **Schutz vor unbefugtem Mithören (M44)**

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

Die übertragenen Funk-Signale bei der Kommunikation mit mobilen Geräten, insbesondere mit Mobiltelefonen, können nicht physikalisch gegen unbefugtes Mithören abgeschirmt werden. Daher dürfen hoch schützenswerte Informationen im Klartext nur übermittelt werden, wenn die Kommunikation verschlüsselt erfolgt. (z. B. verschlüsseltes WLAN).

Bei Telefongesprächen mit vertraulichem Inhalt (z.B. Dienstgeheimnisse) ist darauf zu achten, dass Personen in unmittelbarer Umgebung das Gespräch nicht mithören können.

- **Zugriffsschutz mobiler Geräte (M45)**

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

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

- **Verlust eines mobilen Geräts (M46)**

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

Der Verlust eines mobilen Geräts muss unverzüglich der zuständigen Stelle gemeldet werden. Insbesondere bei Mobiltelefonen müssen Maßnahmen zur Sperrung des Geräts bzw. der SIM-Karte getroffen werden. Weitere Maßnahmen, wie zum Beispiel die Lokalisierung des Geräts, das Absetzen eines Befehls zur Datenlöschung usw. sind – soweit möglich – ebenfalls sofort durchzuführen.

- **Geregelte Übergabe eines mobilen Geräts (M47)**

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

Bei der Nutzung von mobilen PCs durch verschiedene Personen muss die Übergabe

geregelt stattfinden. Dabei muss mindestens nachvollziehbar sein, welche Person das Gerät benutzt hat.

- **Schutz der Daten auf mobilen Geräten (M48)**

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

Schützenswerte Daten dürfen auf mobilen Geräten nur geschützt abgelegt werden. Insbesondere Dokumente und Informationen, deren Schutzbedarf hoch oder sehr hoch ist, müssen vor der Übertragung auf das mobile Gerät verschlüsselt werden. Bei Daten der Schutzklasse sehr hoch darf der für die Entschlüsselung notwendige Schlüssel nicht auf demselben Geräte abgelegt werden.

3.2.7 Zugriffsschutz

Grundsätzlich gilt, dass nur die Personen Zugang zu dem Netz und den damit verfügbaren Ressourcen der Goethe-Universität Frankfurt erhalten, die zuvor die Erlaubnis zur Nutzung von den dafür zuständigen Stellen erhalten haben. Jede Nutzungserlaubnis muss personengebunden sein. Die Verwendung fremder Nutzerkennungen, also anderer als der eigenen, ist nicht erlaubt.

- **Einrichtung anonymer Benutzerkonten (M49)**

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

Anonyme Benutzerkonten sollten nur in begründeten Ausnahmefällen (beispielsweise als Zugang für FTP-Server) erlaubt werden. Wenn in sicherheitsrelevanten Bereichen anonyme Benutzerkennungen eingesetzt werden (z.B. das Benutzerkonto „root“ auf Unix-Systemen), müssen geeignete organisatorische Maßnahmen sicherstellen, dass der Kreis der Berechtigten auf ein absolutes Minimum zu reduzieren und dieser Personenkreis zu dokumentieren ist.

- **Bereitstellung von Verschlüsselungssystemen (M50)**

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

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

- **Netzzugänge (M51)**

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

Der Anschluss von Systemen über die Netzzugänge der Goethe-Universität Frankfurt hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Access Points o.ä.) ist unzulässig.

- **Ausscheiden von Mitarbeitern (M52)**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	Bereichsleitung, Vorgesetzter des ausscheidenden Mitarbeiters, IT-Personal

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass der zuständige IT-Beauftragte bzw. Verfahrensverantwortliche rechtzeitig über das Ausscheiden oder den Wechsel eines Mitarbeiters informiert wird. Die zuständige Organisationseinheit des betreffenden Mitarbeiters hat vor dem Ausscheiden über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung des ausscheidenden Mitarbeiters zugeordnet sind, und deren Übernahme zu organisieren. Vor dem Ausscheiden sind sämtliche Unterlagen, die sicherheitsrelevante Angaben enthalten sowie ausgehändigte Schlüssel zurückzufordern. Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Für eine begrenzte Übergangszeit können die Zugangs- und Zugriffsrechte zur Abwicklung eines geordneten Abschlusses bestehen bleiben. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt, so ist nach dem Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.

- **Personenbezogene Kennungen (M53)**

Verantwortlich für Initiierung:	IT-Beauftragter
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 zum Beispiel mit Benutzerkennung und Passwort oder adäquater Verfahren erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel personenbezogen erfolgen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Zugangsdaten zum Beispiel 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. Die Einrichtung und Freigabe einer Benutzerkennung darf nur in einem bereichsintern geregelten Verfahren erfolgen. Die Einrichtung, Freigabe und Sperrung sind zu dokumentieren.

- **Administratorkennungen (M54)**

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

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

- **Zentralisierung des Identity- und Passwort-Managementsystems (M55)**

Verantwortlich für Initiierung:	Präsidium
Verantwortlich für Umsetzung:	Bereichsleitung, IT-Beauftragter, IT-Personal

Die IT-Dienstleister der Goethe-Universität Frankfurt sind verpflichtet, ein geeignetes

System zur zentralen Identity- und Passwortverwaltung bereit zu stellen. Zur Authentifizierung und Autorisierung müssen alle zugangskontrollierten Systeme das zentral angebotene Identity- und Passwort-Managementsystem nutzen, soweit dies technisch umsetzbar und organisatorisch sinnvoll ist.

- **Passwörter (M56)**

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

Werden in einem IT-System Passwörter zur Authentifizierung 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. Insbesondere darf das Passwort nicht externen Dienstleistern bekannt gegeben werden, zum Beispiel im Rahmen der Nutzung von E-Mail-Sammeldiensten. Idealerweise sollte das Passwort nicht notiert werden. Für die Wahl von Passwörtern gelten folgende Regeln[3]:

- Das Passwort darf nicht leicht zu erraten sein, wie zum Beispiel Benutzername, Vor- oder Nachname, Kfz-Kennzeichen, Geburtsdatum.
- Das Passwort darf nicht aus Wörtern bestehen, die in Wörterbüchern (Passwörterlisten als Grundlage so genannter Wörterbuchangriffe) enthalten sind.
- Das Passwort muss mindestens 5 verschiedene Zeichen enthalten und mindestens zwei Nicht-Buchstaben (Ziffer oder Sonderzeichen) enthalten.
- Das Passwort muss mindestens 8 Zeichen lang und darf nicht länger als die Anzahl der signifikanten Stellen sein.
- Voreingestellte Passwörter (z. B. Standardpasswörter des Herstellers bei Auslieferung von Systemen oder Initialpasswörter) müssen durch individuelle Passwörter ersetzt werden.
- Initialpasswörter müssen unterschiedlich sein und so gewählt werden, dass sie den hier festgelegten Anforderungen genügen.
- Das Passwort muss geheim gehalten werden und darf bei persönlichen Benutzerkennungen nur dem Inhaber der Benutzerkennung selbst bekannt sein.
- Passwörter, die für Systeme und Dienste der Goethe-Universität Frankfurt benutzt werden, dürfen nicht für andere Zwecke verwendet oder auf außeruniversitären Systemen abgelegt werden.
- Ein Passwortwechsel ist sofort durchzuführen, wenn der Verdacht besteht, dass das Passwort unautorisierten Personen bekannt geworden ist oder wenn der Verdacht auf eine System-Kompromittierung besteht. Auch wenn Passwörter versehentlich bei anderen Systemen oder anderen Anbietern von Diensten eingegeben werden, muss das Passwort gewechselt werden. Bei der Abgabe von Rechnern oder Speichermedien, auf denen Passwörter abgelegt sind, müssen dann die betreffenden Passwörter gewechselt werden, wenn eine vorherige Löschung der Passwörter nicht gewährleistet werden

[3] Auf eine Regel zur Begrenzung des Gültigkeitszeitraums eines Passworts wurde verzichtet, da sich in der Praxis gezeigt hat, dass die Passwortsicherheit durch eine Begrenzung der Lebensdauer nicht zwangsläufig erhöht wird.

kann (z.B. bei Abgabe eines Rechners im Reparaturfall).

- Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr verwendet werden.
- Die Eingabe des Passwortes muss unbeobachtet stattfinden.
- Die Passwörter müssen im System zugriffssicher gespeichert werden.

Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern (z.B. "qwertz123" oder "12345678") sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Sofern für die Erstanmeldung neuer Benutzer triviale oder einheitliche Initialpasswörter vergeben werden, muss eine Änderung bei der Erstanmeldung erzwungen werden.
- Erfolgen von einem System zu viele Fehlversuche bei der Eingabe eines Passworts (z.B. 10 Fehlversuche bei manueller Eingabe), sollte das System, von dem die Fehlversuche stammen, temporär oder dauerhaft gesperrt werden.
- Bei der Authentifizierung in vernetzten Systemen dürfen Passwörter nicht unverschlüsselt übertragen werden. Die Systembetreiber haben dafür Sorge zu tragen, dass Authentifizierung nur verschlüsselt erfolgen kann.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

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

- **Zugriffsrechte (Autorisierung) (M57)**

Verantwortlich für Initiierung:	IT-Beauftragter (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.

Die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer erfolgt grundsätzlich auf schriftlichen Antrag bei den zuständigen Verfahrensverantwortlichen.

Es ist zu prüfen, inwieweit die Zugriffserlaubnis von bestimmten IT-Systemen begrenzt werden kann. Für Benutzer mit besonderen Rechten, insbesondere für Administratorkennungen, ist eine Zugriffserlaubnis auf die notwendigen Rechner (i.d.R. sind es der betreffende Server und die Arbeitsplatz-PCs) zu begrenzen.

- **Änderung der Zugriffsrechte (M58)**

Verantwortlich für Initiierung:	IT-Beauftragter (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.

- **Abmelden und ausschalten (M59)**

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

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

- **Verwendung dienstlicher E-Mail-Adressen (M60)**

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

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

3.2.8 Protokollierung

Eine angemessene Protokollierung, Audit und Revision sind wesentliche Faktoren der Netzsicherheit. Die 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.

Bei der Revision werden die beim (Offline-) Audit gesammelten Daten von einem oder mehreren unabhängigen Mitarbeitern überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken.

- **Protokollierung durch Betriebssysteme (M61)**

Verantwortlich für Initiierung:	IT-Beauftragter (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, bei denen die Protokollauswertung Bestandteil der dienstlichen Aufgaben ist. Das Prinzip der Zweckbindung gemäß dem Hessischen Datenschutzgesetz muss beachtet werden.

- **Protokollierung durch Anwendungsprogramme (M62)**

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

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

3.2.9 System- und Netzwerkmanagement

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

Die Netzdokumentation, die bei einer Veröffentlichung die Sicherheit der Netze der Universität gefährden kann (z.B. auf Grund detaillierter Angaben), ist verschlossen zu halten und vor dem Zugriff Unbefugter zu schützen.

- **Sichere Netzwerkadministration (M63)**

Verantwortlich für Initiierung:	IT-Beauftragter, IT-Dienstleister (für dezentrale Bereiche)
Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister (für zentrale Bereiche)

Es muss geregelt und sichergestellt sein, dass die Administration des lokalen Netzwerks nur von dem dafür vorgesehenen Personal durchgeführt wird. Aktive und passive Netzkomponenten sowie Server sind vor dem Zugriff Unbefugter zu schützen. Bereichsübergreifende Netzwerke dürfen ausschließlich nur von Mitarbeitern der zuständigen zentralen Stelle zur Erbringung dieser Infrastrukturleistungen (i.d.R. Hochschulrechenzentrum) administriert und kontrolliert werden.

- **Netzmonitoring (M64)**

Verantwortlich für Initiierung:	IT-Beauftragter, IT-Dienstleister (für dezentrale Bereiche)
Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister (für zentrale Bereiche)

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 (M65)**

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

Es sind alle öffentlich zugänglichen und nicht benötigten Netzwerkzugänge zu deaktivieren oder auf andere geeignete Weise zu schützen, damit ein unbefugter Zugang zum Netz der Goethe-Universität Frankfurt verhindert wird.

Alle nicht mehr benötigten Netzzugänge sind den zuständigen Administratoren unverzüglich zu melden.

- **Kommunikation zwischen unterschiedlichen Sicherheitsniveaus (M66)**

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

Die gesamte Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf darf ausschließlich über kontrollierte Kanäle erfolgen, die durch ein spezielles Schutzsystem geführt werden. Die Installation und der Betrieb anderer Kommunikationsverbindungen neben den Netzverbindungen der Goethe-Universität Frankfurt sind nicht gestattet. Falls auf Grund besonderer Umstände die Installation anderer Kommunikationswege unumgänglich ist, muss dies zuvor durch die zuständige Stelle genehmigt werden.

- **Identifikation von Rechnernamen (M67)**

Verantwortlich für Initiierung:	IT-Beauftragter
Verantwortlich für Umsetzung:	IT-Personal, IT-Dienstleister, Anwender

Zur Erleichterung der Notfallvorsorge und der Missbrauchsnachverfolgung müssen die lokal zuständigen Administratoren geeignete Maßnahmen ergreifen, um am Netzwerk angeschlossene Rechner einem Verantwortlichen zuordnen zu können (z.B. DNS-Einträge, DHCP-Log, RADIUS-Log, Client-Management-System).

3.2.10 Datensicherung

- **Organisation der Datensicherung (M68)**

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 Sicherung erfolgt. Im Falle

personenbezogener Daten sind die geforderten Mindest- bzw. Höchstzeiträume für die Aufbewahrung der Daten zu beachten.

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

- **Durchführung der Datensicherung auf Arbeitsplatz-PCs (M69)**

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

Grundsätzlich sollten Daten auf zentralen Fileservern gespeichert werden. Dort erfolgt turnusmäßig eine zentrale Datensicherung. Wo ein Zugriff auf einen zentralen Fileserver nicht möglich oder gewünscht ist, müssen andere geeignete Maßnahmen zur Datensicherung ergriffen werden. Die Verantwortung hierfür liegt beim Anwender.

- **Durchführung der Datensicherung auf Servern (M70)**

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

Die Sicherung der Daten auf Servern sollte im angemessenen Rhythmus erfolgen. Auch System- und Programmdaten sind nach Veränderungen zu sichern. Zur Datensicherung sind dafür geeignete Backup-Werkzeuge zu verwenden, die eine Datensicherung nach dem Generationenprinzip unterstützen.

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

- **Verifizierung der Datensicherung (M71)**

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

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

3.2.11 Datenträgerkontrolle

- **Aufbewahrung (M72)**

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

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

Bei der Lagerung der Datenträger sind die Angaben der Hersteller, insbesondere zu Temperatur und Luftfeuchtigkeit zu beachten. Bei längerer Lagerung sind Vorkehrungen

zu treffen, die eine alterungsbedingte Zerstörung der Datenträger verhindern. In angemessenen Zeitabständen ist ein Umkopieren der Daten auf neuere Datensicherungsträger vorzusehen. Die Fortentwicklung der Sicherungssysteme ist zu beachten. Bei einer Langzeitarchivierung muss ggf. die Bereitstellung eines Lesegeräts eingeplant werden, das für die verwendeten Datenformate geeignet ist.

- **Weitergabe von Datenträgern mit schützenswerten Daten (M73)**

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

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

- **Gesicherter Transport (M74)**

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

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

- **Reparatur von IT mit Speichermedien (M75)**

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

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

- **Physisches Löschen und Entsorgung von Datenträgern (M76)**

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. Dabei ist auf den Einsatz sicherer Löschverfahren zu achten.

Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden.

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

- **Sichere Entsorgung vertraulicher Papiere (M77)**

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 sind die geltenden Normvorschriften zu beachten. Alternativ kann die Entsorgung auch über einen Dienstleister erfolgen. In diesem Fall muss sichergestellt sein, dass der Auftragnehmer über entsprechende Zertifikate verfügt. Der Auftragnehmer ist zur Protokollierung der Aktenvernichtung zu verpflichten

- **Sicherer Einsatz virtueller IT-Systeme (M78)**

Verantwortlich für die Initiierung: Verfahrensverantwortlicher, IT-Beauftragter
Verantwortlich für die Umsetzung: IT-Personal

Bei der Inbetriebnahme virtueller IT-Systeme müssen einige Besonderheiten beachtet werden, die über die für physische IT-Systeme notwendigen Maßnahmen hinausgehen. Dies resultiert aus der Dynamik und Flexibilität der virtuellen IT-Systeme sowie der Möglichkeit, dass mehrere virtuelle IT-Systeme, die unterschiedliche Daten verarbeiten, auf einem Virtualisierungsserver nebeneinander betrieben werden.

Die Inbetriebnahme virtueller IT-Systeme muss sorgfältig vorbereitet werden. Es sollten insbesondere folgende Punkte vor der unmittelbaren Inbetriebnahme beachtet werden:

- Es muss sichergestellt werden, dass nur die hierfür zuständigen Administratoren die Virtualisierungssoftware bezüglich der virtuellen IT-Systeme konfigurieren sowie virtuelle IT-Systeme einrichten oder löschen können.
- Es muss gewährleistet sein, dass die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur zur Verfügung stehen.
- Werden virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver betrieben, müssen die einzelnen virtuellen IT-Systeme auf einem physischen Server entsprechend der Schutzbedarfsstufe isoliert und gekapselt sein.
- Der Einsatz mehrerer virtueller IT-Systeme auf einem physischen Server kann erhebliche Auswirkungen auf die Verfügbarkeit, den Durchsatz und die Antwortzeiten der betriebenen Anwendungen haben. Es ist zu prüfen, ob die Anforderungen an die Verfügbarkeit und den Durchsatz der Applikationen mit der eingesetzten Virtualisierungslösung erfüllt werden können.
- Weiterhin sollen die Leistungseigenschaften virtueller Server überwacht werden, damit bei Engpässen zeitnah Anpassungen der Konfiguration vorgenommen werden können. Die Überwachung kann auf der Ebene der virtuellen IT-Systeme oder auf der Ebene des jeweiligen Virtualisierungsservers erfolgen.

4. Feststellung des Schutzbedarfs

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

Die Untersuchung eines IT-Verfahrens beginnt mit der Analyse des Schutzbedarfes der im IT-Verfahren verarbeiteten Daten. Der Schutzbedarf wird durch die drei Werte (Schutzklassen) „normal“, „hoch“ und „sehr hoch“ klassifiziert. Die folgenden Tabellen beschreiben die Bedeutung dieser Werte in Hinblick auf verschiedene Kriterien. Für jedes IT-Verfahren ist ein Mindestmaß an Sicherheit zu gewährleisten, daher sind die Regeln des IT-Grundschutzes in allen IT-Verfahren verpflichtend einzuhalten. Aufgrund des Ergebnisses der Schutzbedarfsanalyse können sich darüberhinausgehende Anforderungen ergeben.

Wird als Ergebnis der Schutzbedarfsanalyse das IT-Verfahren in die Schutzklasse „normal“ eingestuft, reichen im Allgemeinen die Maßnahmen des IT-Grundschutzes aus. In allen anderen Fällen, also wenn das IT-Verfahren in die Schutzklasse „hoch“ oder „sehr hoch“ eingestuft wird, muss eine verfahrensspezifische Risikoanalyse durchgeführt werden. Die Vorgehensweise bei einer Risikoanalyse wird in dem folgenden Kapitel 5 beschrieben.

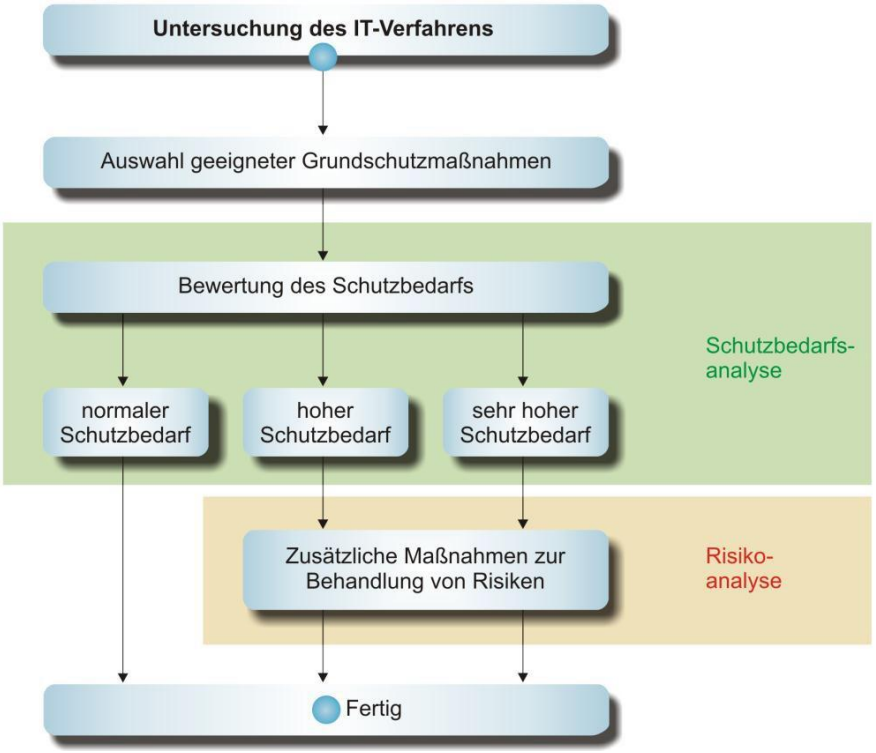

Abbildung 2: Vereinfachte Darstellung der sich aus der Schutzbedarfsanalyse ergebenden Konsequenzen.

4.1 Schutzbedarfsanalyse

Die folgende Beschreibung gliedert sich in zwei Abschnitte. Im ersten Abschnitt wird die Vorgehensweise dargestellt. Der zweite Abschnitt beinhaltet Tabellen, mit deren Hilfe eine Bewertung des Schutzbedarfs erfolgen soll.

4.1.1 Vorgehensweise

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

- Beeinträchtigung des informationellen Selbstbestimmungsrechts
- Beeinträchtigung der persönlichen Unversehrtheit
- Beeinträchtigung der Aufgabenerfüllung
- Negative Außenwirkung
- Finanzielle Auswirkungen
- Verstoß gegen Gesetze, Vorschriften und Verträge

Die Durchführung einer Schutzbedarfsanalyse unter Anwendung der unter 4.1.2 aufgeführten Tabellen wird im Folgenden kurz skizziert. Dabei werden die durchzuführenden Schritte erläutert und mit Auszügen aus einer fiktiven Beispielanalyse illustriert.

Auf Grund der gewonnenen Erfahrungen wird empfohlen, die Schutzbedarfsanalyse in einem Team durchzuführen.

1. Schritt: Identifikation der zu schützenden Daten

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

Beispiel:

1. *Vorname*
2. *Nachname*
3. *Straße mit Hausnummer*
4. *Postleitzahl und Ort*
5. *Fachbereichszugehörigkeit*
6. *Studiengang*
7. *Prüfungsergebnisse*
8. *Belegte Seminare*

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

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

Beispiel:

1. *Name (Vorname, Nachname)*
2. *Adresse (Straße mit Hausnummer, Postleitzahl und Ort)*
3. *Fachbereichszugehörigkeit*
4. *Studiengang*
5. *Prüfungsergebnisse*
6. *Belegte Seminare*

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

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

Beispiele Vertraulichkeit:

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

⇨ *Der Umgang mit Kollegen kann beeinträchtigt werden. Der berufliche Werdegang kann erheblich beeinträchtigt werden.*

Angenommen, Unbefugte erlangen Kenntnis von den Personaldaten: Welche Folgen hätte dies im schlimmsten Falle für die persönliche Unversehrtheit?

⇨ *Keine, Folgen für die Gesundheit können ausgeschlossen werden.*
(…)

Beispiel Integrität:

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

⇨ *Die Goethe-Universität Frankfurt würde als unzuverlässige Organisation angesehen werden. Es muss von einem überregionalen (bundesweiten) Ansehensverlust ausgegangen werden.*
(…)

Beispiel Verfügbarkeit:

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

⇨ *Es kommt zu Verzögerungen bei der Auszahlung der Bezüge. Die beschäftigten Mitarbeiter müssen mit Abschlagszahlungen rechnen.*
(…)

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

4. Schritt: Einordnung in eine der drei Schutzbedarfskategorien normal / hoch / sehr hoch

Die in den Gedankenexperimenten festgestellten schlimmsten Folgen müssen anhand der in den folgenden Tabellen vorgegebenen Maßstäben (normal / hoch / sehr hoch) eingestuft werden. Das Ergebnis muss dokumentiert werden. Das Maximum des höchsten Schutzbedarfs einer Kategorie bestimmt den Schutzbedarf des IT-Verfahrens (MaximumPrinzip).

Beispiel:
In der folgenden Beispieltabelle würde das IT-Verfahren in die Schutzklasse „hoch“ eingestuft werden.

Beispiel Vertraulichkeit:

Tabelle 2: Verlust von Vertraulichkeit

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

4.1.2 Bewertungstabellen

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

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

4.1.2.1 Verlust von Vertraulichkeit

Tabelle 3: Verlust von Vertraulichkeit				
Schadenskategorien	**Bedrohung**	**Abschätzung des Schadens**		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Bekannt werden der Daten für Unbefugte ...	... kann für die Betroffenen 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.	… kann für die Betroffenen möglicherweise zu einer erheblichen Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.	... kann für die Betroffenen möglicherweise zu einer gravierenden Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit	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.
Beeinträchtigung der Aufgabenerfüllung	Die Kenntnisnahme der Daten durch Unbefugte ...	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit (z.B. Arbeitsgruppe) geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit (z.B. Fachbereiche, Teilbereiche der Universitätsverwaltung) ist unwesentlich beeinträchtigt.	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit (z.B. Arbeitsgruppe) erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit (z.B. Fachbereiche, Teilbereiche der Universitätsverwaltung) ist wesentlich beeinträchtigt.	... gefährdet die Aufgabenerfüllung der Goethe-Universität Frankfurt. Kernprozesse der Universität können massiv behindert werden.
Negative Außenwirkung	Missbrauch der Daten ...	…führt höchstens zu geringem Ansehensverlust eines Teilbereichs der GU bei einer eingeschränkten Öffentlichkeit.	... führt zu einem Ansehensverlust der GU bei einer eingeschränkten Öffentlichkeit oder einem hohen Ansehensverlust eines Teilbereichs der Goethe-Universität.	... führt zu einem Ansehensverlust der GU in der breiten Öffentlichkeit.
Finanzielle Auswirkungen	Missbrauch der Daten	Summe der finanziellen Auswirkungen < 150.000 €	Summe der finanziellen Auswirkungen < 3.000.000 €	Summe der finanziellen Auswirkungen >= 3.000.000 €
daraus resultierender Schutzbedarf:		**normal**	**hoch**	**sehr hoch**

Tabelle 3: Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren. Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“. Die in der Zeile „Finanzielle Auswirkungen“ angegebenen Beträge wurden in Abhängigkeit von der Höhe des Haushalts der Goethe-Universität Frankfurt festgelegt.

4.1.2.2 Verlust von Integrität

Tabelle 4: Verlust von Integrität				
Schadenskategorien	**Bedrohung**	**Abschätzung des Schadens**		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Unberechtigte Veränderung der Daten ...	... kann für die Betroffenen 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.	… kann für die Betroffenen möglicherweise zu einer erheblichen Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.	... kann für die Betroffenen möglicherweise zu einer gravierenden Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit	Unberechtigte Veränderung der Daten ...	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen Unversehrtheit.	... führt zu erheblicher Beeinträchtigung der persönlichen Unversehrtheit.	... bedroht die Existenz des Betroffenen.
Beeinträchtigung der Aufgabenerfüllung	Unberechtigte Veränderung der Daten ...	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit (z.B. Arbeitsgruppe) geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit (z.B. Fachbereiche, Teilbereiche der Universitätsverwaltung) ist unwesentlich beeinträchtigt.	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit (z.B. Arbeitsgruppe) erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit (z.B. Fachbereiche, Teilbereiche der Universitätsverwaltung) ist wesentlich beeinträchtigt.	... gefährdet die Aufgabenerfüllung der Goethe-Universität Frankfurt. Kernprozesse der Universität können massiv behindert werden.
Negative Außenwirkung	Unberechtigte Veränderung der Daten ...	…führt höchstens zu geringem Ansehensverlust eines Teilbereichs der GU bei einer eingeschränkten Öffentlichkeit	... führt zu einem Ansehensverlust der GU bei einer eingeschränkten Öffentlichkeit oder einem hohen Ansehensverlust eines Teilbereichs der Goethe-Universität	... führt zu einem Ansehensverlust der GU in der breiten Öffentlichkeit.
Finanzielle Auswirkungen	Unberechtigte Veränderung der Daten ...	Summe der finanziellen Auswirkungen < 150.000 €	Summe der finanziellen Auswirkungen < 3.000.000 €	Summe der finanziellen Auswirkungen >= 3.000.000 €
daraus resultierender Schutzbedarf:		**Normal**	**hoch**	**sehr hoch**

Tabelle 4: Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren. Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“. Die in der Zeile „Finanzielle Auswirkungen“ angegebenen Beträge wurden in Abhängigkeit von der Höhe des Haushalts der Goethe-Universität Frankfurt festgelegt.

4.1.2.3 Verlust von Verfügbarkeit

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

Tabelle 5: Verlust von Verfügbarkeit

Schadenskategorien	Bedrohung	Abschätzung des Schadens		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Verlust der Daten ...	... kann für die Betroffenen 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.	… kann für die Betroffenen möglicherweise zu einer erheblichen Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.	... kann für die Betroffenen möglicherweise zu einer gravierenden Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
Beeinträchtigung der persönlichen Unversehrtheit	Verlust der Daten ...	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen Unversehrtheit.	... führt zu erheblicher Beeinträchtigung der persönlichen Unversehrtheit.	... bedroht die Existenz des Betroffenen.
Beeinträchtigung der Aufgabenerfüllung	Verlust der Daten ...	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit (z.B. Arbeitsgruppe) geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit (z.B. Fachbereiche, Teilbereiche der Universitätsverwaltung) ist unwesentlich beeinträchtigt.	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit (z.B. Arbeitsgruppe) erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit (z.B. Fachbereiche, Teilbereiche der Universitätsverwaltung) ist wesentlich beeinträchtigt.	... gefährdet die Aufgabenerfüllung der Goethe-Universität Frankfurt. Kernprozesse der Universität können massiv behindert werden.
Negative Außenwirkung	Verlust der Daten ...	…führt höchstens zu geringem Ansehensverlust eines Teilbereichs der GU bei einer eingeschränkten Öffentlichkeit	... führt zu einem Ansehensverlust der GU bei einer eingeschränkten Öffentlichkeit oder einem hohen Ansehensverlust eines Teilbereichs der Goethe-Universität	... führt zu einem Ansehensverlust der GU in der breiten Öffentlichkeit.
Finanzielle Auswirkungen	Verlust der Daten ...	Summe der finanziellen Auswirkungen < 150.000 €	Summe der finanziellen Auswirkungen < 3.000.000 €	Summe der finanziellen Auswirkungen >= 3.000.000 €
daraus resultierender Schutzbedarf:		**Normal**	**hoch**	**sehr hoch**

Tabelle 5: Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren. Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“. Die in der Zeile „Finanzielle Auswirkungen“ angegebenen Beträge wurden in Abhängigkeit von der Höhe des Haushalts der Goethe-Universität Frankfurt festgelegt.

4.1.2.4 Verstöße gegen Gesetze, Vorschriften und Verträge

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

Datenschutzgesetze, beispielsweise

- Hessisches Datenschutzgesetz (HDSG)
- Bundesdatenschutzgesetz (BDSG)

Hochschulgesetze bzw. -verordnungen, beispielsweise

- Hessisches Hochschulgesetz (HSchulG HE)
- Hessische Immatrikulationsverordnung (HImmaVO)
- Hessisches Beamtengesetz (HBG)

Vorschriften zur Mitbestimmung, beispielsweise

- Hessisches Personalvertretungsgesetz
- Tarifvertrag über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informationstechnik

Tabelle 6: Verstoß gegen Gesetze, Vorschriften und Verträge

Bedrohung	**Abschätzung des Schadens**		
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 gegen Gesetze oder Vorschriften mit schwerwiegenden rechtlichen Konsequenzen. … hat Vertragsverletzungen zur Folge, deren Haftungsschäden für die GU ruinös sind.
Unberechtigte Veränderung der Daten …			
Verlust der Daten …			
daraus resultierender Schutzbedarf:	**normal**	**hoch**	**sehr hoch**

Tabelle 6: Bewertungsmaßstab für den Schutzbedarf von IT-Verfahren. Die dreifache vertikale Linie symbolisiert die Grenze zwischen „Grundschutzmaßnahmen reichen aus“ bzw. „reichen nicht aus“.

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

5. Risikoanalyse

In diesem Abschnitt wird der Zweck einer Risikoanalyse erläutert und die Vorgehensweise nach einer bewährten Methode skizziert. Anschließend wird die Dokumentation einer Risikoanalyse anhand eines Beispiels gezeigt.

Zur Durchführung einer Risikoanalyse existieren verschiedene Methoden. Die hier vorgestellte Methode orientiert sich an dem Sicherheitshandbuch des BSI. Zur Risikoanalyse kann in Absprache mit dem Sicherheitsmanagement-Team auch alternativ eine andere anerkannte Methode angewendet werden.

5.1 Ziel der Risikoanalyse

In der in Kapitel 4 beschriebenen Schutzbedarfsanalyse wurde – unabhängig von bereits getroffenen Maßnahmen – die mögliche Schadenshöhe abgeschätzt („worst case"-Analyse). Für jedes IT-Verfahren mit hohem oder sehr hohem Schutzbedarf (Schadensstufe „hoch" und „sehr hoch") muss in einem zweiten Schritt eine Risikoanalyse durchgeführt werden. Die dabei ermittelten untragbaren Risiken müssen durch geeignete Vorkehrungen und Maßnahmen auf ein tragbares Maß reduziert werden, d. h. die Wahrscheinlichkeit des Schadenseintritts und damit das Risiko muss verringert werden. Die Ergebnisse sind in geeigneter Weise zu dokumentieren.

5.2 Definition Risiko

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

Für die Abschätzung, mit welcher Wahrscheinlichkeit ein Schaden zu erwarten ist, wird eine Skala mit Werten von „häufig" bis „praktisch nie" verwendet. Dabei werden den Werten die in der folgenden Tabelle aufgeführten Bedeutungen unterlegt.

Häufigkeit	Bedeutung
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. Stromausfall)
öfter	Das Schadensereignis tritt alle paar Monate einmal auf (z.B. versehentliches Löschen von Daten)
häufig	Das Schadensereignis tritt alle paar Wochen einmal auf (z.B. Fehlbedienung)

Tabelle 7: Häufigkeitswerte der Eintrittswahrscheinlichkeit von Schäden

Es wird unterschieden zwischen den zwei Risikoklassen „tragbar“ und „untragbar“. Die Zuordnung von Risiken zu einer bestimmten Risikoklasse erfolgt anhand der nachstehenden Tabelle 8. Dabei bedeuten

Untragbar – untragbares Risiko,

Tragbar – noch tragbares Risiko.

Schadenshöhe Häufigkeit	**normal** **1**	**Hoch** **2**	**sehr hoch** **3**
praktisch nie	Tragbar	Tragbar	Tragbar
sehr selten	Tragbar	Tragbar	**Untragbar**
selten	Tragbar	**Untragbar**	**Untragbar**
öfter	**Untragbar**	**Untragbar**	**Untragbar**
häufig	**Untragbar**	**Untragbar**	**Untragbar**

Tabelle 8: Risikoklassen

5.3 Vorgehensweise

Die 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 auf diese Objekten wirken können. Die daraus resultierenden Schäden werden nach der im Kapitel 4 verwendeten dreiteiligen Werteskala (normal, hoch, sehr hoch) klassifiziert. Danach wird mit Hilfe der Tabelle 7 abgeschätzt, mit welcher Häufigkeit ein Schaden in dieser Höhe zu erwarten ist. Anhand der Tabelle 8 können die ermittelten Risiken einer Risikoklasse zugeordnet werden.

Untragbare Risiken müssen durch zusätzliche Maßnahmen auf das für die Goethe-Universität Frankfurt tragbare Maß reduziert werden. Bei der Risikoanalyse wird vorausgesetzt, dass die im Kapitel IT-Grundschutzes vorgesehenen Maßnahmen auch für das betreffende IT-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. 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 Goethe-Universität Frankfurt ist.

Zusammenfassend sind folgende Schritte für die Risikoanalyse durchzuführen:

Schritt 1: Erfassung der für den Geschäftsprozess bzw. das IT-Verfahren benötigten Objekte

Schritt 2: Bewertung des Schutzbedarfs der Objekte
Hilfsmittel: Bewertungstabellen (Abschnitt 4.1.2)

Schritt 3: Bestimmung der Häufigkeit von Schäden
Hilfsmittel: Tabelle der Häufigkeitswerte (Seite 54)

Schritt 4: Zusammenstellung und Bewertung (Klassifizierung) der Risiken
Hilfsmittel: Tabelle der Risikoklassen (Seite 55)

Schritt 5: Maßnahmen zur Reduzierung der untragbaren Risiken

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

5.4 Beispiel

Anhand des folgenden fiktiven Beispiels wird gezeigt, wie die Ergebnistabellen aussehen können. Das Beispiel umfasst nur eine Auswahl von möglichen Bedrohungen nebst Bewertungen und Maßnahmen. Wie aus dem Beispiel ersichtlich, können auch bei tragbaren Risiken zusätzliche Maßnahmen ergriffen werden, wenn damit die Grundsätze der Wirtschaftlichkeit nicht verletzt werden. Bei der Wahl geeigneter Maßnahmen zur Risikobeherrschung können die IT-Grundschutzkataloge des BSI hilfreich sein. Insbesondere enthalten die Kataloge eine umfangreiche Sammlung von Sicherheitsmaßnahmen zu einer Vielzahl technischer IT-Systeme.

Das Ergebnis der fiktiven Risikoanalyse ist in diesem Beispiel in sieben Kategorien (= 7 Tabellen) dokumentiert:

1. Hardware
2. Infrastruktur
3. Kommunikation
4. Datenträger
5. Software, Daten
6. Papier
7. Personen

Die in der Spalte „Schadenshöhe“ angegebenen Werte sind folgendermaßen zu verstehen:

1 bedeutet Schutzbedarfskategorie „normal“

2 bedeutet Schutzbedarfskategorie „hoch“

3 bedeutet Schutzbedarfskategorie „sehr hoch“

Objektkategorie: Hardware						
Bezeichnung der Bedrohung	Grund-bedro-hung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Technisches Versagen	Verfügb.	Produktivsysteme	3	sehr selten	**Un-trag-bar**	M-01: Wartungsvertrag Produktivsystem
	Verfügb.	Weitere Server	2	sehr selten	Trag-bar	M-02: Wartungsvertrag weitere Server
	Verfügb.	Arbeitsplatz-PCs	1	selten	Trag-bar	
	Verfügb.	Drucker	1	selten	Trag-bar	
	Verfügb.	Zentrale Netzwerkkom-Ponenten	2	selten	**Un-trag-bar**	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Diebstahl	Verfügb. Vertraul.	Server	2	selten	**Un-trag-bar**	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude M-14: Zugriffsschutz Server
Spannungsschwan-kungen, Blitzschlag	Verfügb.	Produktivsystem	2	sehr selten	Trag-bar	M-07: Unterbrechungsfreie Stromversorgung
	Verfügb.	Weitere Server	1	sehr selten	Trag-bar	M-07: Unterbrechungsfreie Stromversorgung
Fehlbedienung	Vertraul. Integrit.		1	sehr selten	Trag-bar	
Sabotage	Verfügb.	Produktivsystem	1	sehr selten	Trag-bar	
	Verfügb.	Weitere Server	1	sehr selten	Trag-bar	
Unkontrollierter Zu-gang	Verfügb. Integrit. Vertraul.	Zentrale Server	2	selten	**Un-trag-bar**	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude M-14: Zugriffsschutz Server
	Integrit. Vertraul.	Clients	2	selten	**Un-trag-bar**	M-08: Zugangsschutz Cli-ents

Tabelle 9: Ergebnis der fiktiven Risikoanalyse für die Kategorie Hardware.

Objektkategorie: Infrastruktur						
Bezeichnung der Bedrohung	Grund-bedro-hung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Höhere Gewalt, Ter-ror, Vandalismus	Verfügb.	Serverraum	1	prak-tisch nie	Trag-bar	
	Verfügb.	Zentrale Netzkompo-Nenten	1	sehr selten	Trag-bar	

Feuer	Verfügb.	Serverraum	1	sehr selten	Trag-bar	
	Verfügb.	Netzkomponenten	1	sehr selten	Trag-bar	
Wasser	Verfügb.	Serverraum	1	sehr selten	Trag-bar	
	Verfügb.	Netzkomponenten	1	sehr selten	Trag-bar	
Überhitzung	Verfügb.	Serverraum	1	öfter	**Un-trag-bar**	M-09: Klimatisierung
Ausfall der Stromver-sorgung	Verfügb.	Zentrale Hardware	1	sehr selten	Trag-bar	M-07: Unterbrechungsfreie Stromversorgung
Unbefugter Zugang	Vertraul.	Serverraum	2	sehr selten	Trag-bar	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude
	Vertraul.	Arbeitsräume	1	selten	Trag-bar	M-10: Nicht öffentliche Räume

Tabelle 10: Ergebnis der fiktiven Risikoanalyse für die Kategorie Infrastruktur.

Objektkategorie: Kommunikation						
Bezeichnung der Bedrohung	Grund-bedro-hung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Ausfall	Verfügb.	Netzwerk	2	sehr selten	Trag-bar	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Überlastung	Verfügb.	Netzwerk	1	selten	Trag-bar	
Abhören	Vertraul.	Netzwerk	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung
Manipulation	Vertraul. Integrit.	Netzwerk	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung
Anschließen zusätzli-cher Endgeräte	Vertraul. Integrit.	Personenbezogene Daten	2	selten	**Un-trag-bar**	M-11: Abgeschottetes Netz, Zugangsschutz Netzkomponenten
Unerlaubter Zugang	Vertraul. Integrit.	Netzwerk	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung

Tabelle 11: Ergebnis der fiktiven Risikoanalyse für die Kategorie Kommunikation.

Objektkategorie: Datenträger						
Bezeichnung der Bedrohung	Grund-bedro-hung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Unkontrollierter Zu-Griff	Verfügb. Integrit. Vertraul.	Sicherungsbänder	2	sehr selten	Trag-bar	M-12: Verschlüsselung der Datensicherung, Zu-gangsschutz
Beschädigung	Verfügb. Integrit.	Sicherungsbänder	1	sehr selten	Trag-bar	
	Verfügb. Integrit.	Festplatten	1	sehr selten	Trag-bar	M-13: Redundante Spei-chersysteme, Spie-gelplatten
Fehlerhafte Erzeu-Gung	Verfügb. Integrit.	Datenträger	1	sehr selten	Trag-bar	
Unzureichende Ent-sorgung	Vertraul.	Datenträger	2	prak-tisch nie	Trag-bar	
Diebstahl	Verfügb. Vertraul.	Datenträger	3	sehr selten	**Un-trag-bar**	M-12: Verschlüsselung der Datensicherung, Zu-gangsschutz

Tabelle 12: Ergebnis der fiktiven Risikoanalyse für die Kategorie Datenträger.

Objektkategorie: Software, Daten						
Bezeichnung der Bedrohung	Grund-bedro-hung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Unerlaubtes Aufspie-len von Software	Verfügb.	Software, Daten	1	sehr selten	Trag-bar	M-14: Zugriffsschutz Server
Fehlbedienung	Verfügb. Integrit. Vertraul.	Betriebssystem, Daten-Bank	1	sehr selten	Trag-bar	
Unerlaubter Zugriff und Einblick	Integrit. Vertraul.	Datenbank, Daten, Passwörter	2	sehr selten	Trag-bar	M-06: Zugangsschutz Ser-verraum, gesichertes Gebäude M-14: Zugriffsschutz Server
Mangelhafte Verwal-tung der Zugriffs-rechte	Integrit. Vertraul.	Datenbank	2	selten	**Un-trag-bar**	M-15: Rollentrennung
Schadprogramme (Computerviren)	Verfügb. Integrit.	Betriebssystem	1	sehr selten	Trag-bar	
	Vertraul. Integrit.	Clients	1	öfter	**Un-trag-bar**	M-16: Virenscanner

Tabelle 13: Ergebnis der fiktiven Risikoanalyse für die Kategorie Software, Daten.

Objektkategorie: Papier						
Bezeichnung der Bedrohung	Grund-bedro-hung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Unvollständigkeit, mangelnde Aktualität	Verfügb.	Systemdokumentation	1	sehr selten	Trag-bar	
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Trag-bar	
Unzureichende Ent-Sorgung	Vertraul.	Systemdokumentation	1	sehr selten	Trag-bar	
	Vertraul.	Personenbezogene Daten	2	selten	**Un-trag-bar**	M-17: Schredder
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Trag-bar	

Tabelle 14: Ergebnis der fiktiven Risikoanalyse für die Kategorie Papier.

Objektkategorie: Personen						
Bezeichnung der Bedrohung	Grund-bedro-hung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Ausfall	Verfügb.	Administratoren, Appli-Kationsbetreuer	2	selten	**Un-trag-bar**	M-18: Vertretung
Unkenntnis	Verfügb. Integrit. Vertraul.	Administratoren, Appli-Kationsbetreuer	1	sehr selten	Trag-bar	
	Integrit. Vertraul.	Anwender	1	sehr selten	Trag-bar	
Überlastung	Verfügb. Integrit. Vertraul.	Administratoren, Appli-Kationsbetreuer	2	sehr selten	Trag-bar	M-15: Rollentrennung M-18: Vertretung
	Integrit. Vertraul.	Anwender	1	sehr selten	Trag-bar	
Fehlende Kontrollen und Regelungen	Verfügb. Integrit. Vertraul.	Administratoren, Appli-Kationsbetreuer	2	selten	**Un-trag-bar**	M-19: Kontrolle der Akteure
	Integrit. Vertraul.	Anwender	2	sehr selten	Trag-bar	M-19: Kontrolle der Akteure
Nachlässige Pass-worthandhabung	Vertraul.	Passwörter	2	sehr selten	Trag-bar	M-20: Festlegung der Passwortregeln
Kriminelle Absicht	Verfügb. Integrit. Vertraul.	Administratoren, Appli-kationsbetreuer, An-wender	2	sehr selten	Trag-bar	M-15: Rollentrennung M-21: Kontrolle der Proto-koll-Dateien
	Verfügb. Integrit. Vertraul.	Externe	2	sehr selten	Trag-bar	M-11: Abgeschottetes Netz, Verschlüsselung M-06: Zugangsschutz M-14: Zugriffsschutz

Tabelle 15: Ergebnis der fiktiven Risikoanalyse für die Kategorie Personen.

Die in der rechten Tabellenspalte aufgeführten Maßnahmen müssen im Anschluss unter dem jeweiligen Stichwort (z.B.: „M-01: Wartungsvertrag Produktivsystem“) einzeln erläutert werden. Beispielhaft werden nachfolgend drei Maßnahmen wiedergegeben. Ebenso wie bei den vorangegangenen Tabellen handelt es sich um fiktive Beispiele.

M-01: Wartungsvertrag Produktivsystem

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

M-02: Wartungsvertrag weitere Server[4]

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

(…)

M-06: Zugangsschutz Serverraum, gesichertes Gebäude

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

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

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

[4] Es können zusätzliche Maßnahmen ohne zwingende Notwendigkeit ergriffen werden, soweit es wirtschaftlich vertretbar ist.

6. Umsetzung der IT-Sicherheitsrichtlinie

Aufgrund der hohen Eigenständigkeit der einzelnen Organisationseinheiten wird – in Übereinstimmung mit Abschnitt 2.3 „Verantwortlichkeiten und Organisation der IT-Sicherheit“ – die Verantwortung für die Umsetzung der IT-Sicherheitsrichtlinie auf die einzelnen Organisationseinheiten übertragen. Wesentliche Impulse zur Unterstützung der Verantwortlichen sollen dabei von den IT-Beauftragten ausgehen.

6.1 Inkraftsetzung und Aktualisierung der IT-Sicherheitsrichtlinie

Das Präsidium der Goethe-Universität Frankfurt setzt die IT-Sicherheitsrichtlinie in Kraft.

Für neu einzurichtende IT-Verfahren gilt die Sicherheitsrichtlinie ab ihrem Inkrafttreten.
Nach Inkrafttreten der Sicherheitsrichtlinie ist jedes bestehende IT-Verfahren der Goethe-Universität dem Sicherheitsmanagement-Team (SMT) über dessen Vorsitz entsprechend des Anzeigeformulars (Anlage 1) innerhalb von drei Monaten anzuzeigen. Die bestehenden IT- Verfahren sind innerhalb von 2 Jahren nach Inkrafttreten an die Vorgaben der Sicherheitsrichtlinie anzupassen. Nach einem Jahr ist ein Zwischenbericht über das Anpassungsverfahren an den Vorsitz des SMT vorzulegen. In begründeten Fällen kann auf schriftlichen Antrag die Anpassungsphase nach zwei Jahren höchstens um ein weiteres Jahr verlängert werden.
Das Sicherheitsmanagement-Team berichtet dem Präsidium jährlich über Erfahrungen mit der Umsetzung der IT-Sicherheitsrichtlinie.

Die IT-Sicherheitsrichtlinie bedarf der regelmäßigen Überprüfung und Überarbeitung. Die Gewährleistung der Aktualität wird durch die folgende Vorgehensweise sichergestellt:

1.	Beauftragung	Das Präsidium der Goethe-Universität Frankfurt beauftragt das SMT (das Sicherheitsmanagement-Team) mit der Pflege und Fortschreibung der IT-Sicherheitsrichtlinie.
2.	Entwurf einer neuen Richtlinie	Das SMT überarbeitet die Richtlinie und erstellt einen Entwurf einer neuen IT-Sicherheitsrichtlinie.
3.	Abstimmung	Das SMT stimmt den Entwurf mit Datenschutzbeauftragten, IT-Beauftragten und ggf. der Personalvertretung ab.
4.	Vorlage im Präsidium	Das SMT legt dem Präsidium den abgestimmten Richtlinienentwurf vor.
5.	Prüfung und Inkraftsetzung	Das Präsidium prüft den Entwurf und setzt ihn in Kraft.

6.2 Information über die IT-Sicherheitsrichtlinie

Alle Nutzer von IT-Ressourcen der Goethe-Universität Frankfurt müssen über die für sie relevanten Teile der IT-Sicherheitsrichtlinie informiert werden. Neue Mitglieder der Goethe-Universität Frankfurt müssen auf die geltende IT-Sicherheitsrichtlinie beim Eintritt in die Universität hingewiesen werden. Nicht-Mitglieder, die IT-Ressourcen der Goethe-Universität Frankfurt nutzen, müssen von der beauftragenden oder einladenden GU-Stelle auf die für sie relevanten Teile der IT-Sicherheitsrichtlinie nachweislich hingewiesen werden. Die beauftra-

gende oder einladende GU-Stelle hat für die Durchsetzung der IT-Sicherheitsrichtlinie zu sorgen. Insbesondere ist zu gewährleisten, dass

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

als bekannt voraus gesetzt werden können.

6.3 Konfliktlösung bei der Umsetzung der IT-Sicherheitsrichtlinie

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

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

6.4 Leitlinienfunktion für andere Dokumente

Die in dieser Richtlinie enthaltenen Regelungen müssen bei der Ausarbeitung von speziellen IT-Regelwerken, wie Anleitungen, Benutzungsordnungen u. ä. berücksichtigt werden. Insbesondere dürfen Regelungen in anderen Dokumenten den Regeln der IT-Sicherheitsrichtlinie nicht zuwiderlaufen.

7. Glossar

Administrator
Konfiguriert und betreibt IT-Systeme

Anwender
Endbenutzer von IT-Systemen

Anwenderbetreuer
Fungiert als erster Ansprechpartner für Anwender; i.d.R. zuständig für die Installation und Wartung von Endgeräten und Anwendungssoftware

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

Applikationsbetreuer
Betreut Anwendungssoftware und sorgt für deren ordnungsgemäßen Betrieb

Arbeitsplatz-PC, Arbeitsplatz-Rechner
Endgerät für die Aufgaben des Anwenders

Auftragsdatenverarbeitung
Verarbeitung von Daten im Auftrag durch andere Stellen. Für die Verarbeitung personenbezogener Daten im Auftrag gilt §4 HDSG.

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.

Authentizität
Daten können jederzeit ihrem Ursprung zugeordnet werden

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.

Bereichsleitung
Leitungen der Fachbereiche, wissenschaftlichen, zentralen und sonstigen Einrichtungen

Betriebshandbuch

In einem Betriebshandbuch sind (alle) Maßnahmen beschrieben, die für den Betrieb eines IT-Systems notwendig sind.

Betriebssystem

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

BSI

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

Cloud

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Für die Nutzer bleibt die bereitgestellte IT-Infrastruktur verborgen.

Datenschutz

Regelungen und Maßnahmen für die Verarbeitung personenbezogener Daten und deren Schutz vor missbräuchlicher Verarbeitung

Datensicherheit

Sicherstellung von Integrität, Vertraulichkeit und Verfügbarkeit von Daten

Datensicherung

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

Datenträger

Medium zum Speichern der Daten wie Magnetband, Festplatte, CD-ROM, DVD oder USB-Stick.

Datenvermeidung und -sparsamkeit

Personenbezogene Daten dürfen nicht über das notwendige Maß hinaus verarbeitet oder gespeichert werden.

Dienst

(auch Service) ist die Bereitstellung einer Funktionalität zu einer zusammengehörenden Themengruppe (z. B. E-Mail, Webserver, PC-Pool).

Dienstleister

Stellt eine oder mehrere IT-Dienstleistungen zur Verfügung.

E-Mail

Ist ein Verfahren zum elektronischen Versenden und Empfangen von Texten und Dateien. Der Transport erfolgt standardmäßig unverschlüsselt (analog zur Postkarte).

Endgerät

Gerät (zum Beispiel PC oder Telefon), welches an ein Daten- oder Telekommunikationsnetz angeschlossen ist.

Erforderlichkeit von Daten

Personenbezogene Daten dürfen nicht über das notwendige Maß hinaus verarbeitet oder gespeichert werden.

Firewall

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

Geschäftsprozess

Abfolge von zusammenhängenden IT-gestützten Prozessen

HRZ

Hochschulrechenzentrum

Informationelles Selbstbestimmungsrecht

Betroffene haben das Recht, selbst über die Preisgabe und Verwendung ihrer Daten zu entscheiden.

Informationssicherheit

Sicherstellung von Integrität, Vertraulichkeit und Verfügbarkeit von Informationen.

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.

Intervenierbarkeit

Die Technik muss es ermöglichen, dass die Rechte von Betroffenen jederzeit gewahrt werden können.

IT

Informationstechnik (IT) ist ein Oberbegriff für die Informations- und Datenverarbeitung sowie für die dafür benötigte Hard- und Software.

IT-Arbeitsplatz

Arbeitsplatz an dem Informationstechnik eingesetzt wird.

IT-Arbeitsprozess

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

IT-Beauftragter

Ist gleich der dezentrale IT-Sicherheitsbeauftragte gemäß §§ 4 Abs.2, 6 Abs.3 IT-SO

IT-Grundschutz

Zur Sicherstellung eines Grundschutzes wird allen Nutzern von IT-Ressourcen der Goethe-Universität Frankfurt ein einheitlicher Katalog von Sicherheitsmaßnahmen im Umgang mit Informationstechnik vorgeschrieben.

IT-Grundschutzhandbuch

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

IT-Personal

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

IT-Ressourcen

(Informationstechnisches) Mittel für einen Vorgang bzw. zum Handlungsablauf. In der Regel wird unter einer IT-Ressource ein informationstechnisches Betriebsmittel oder IT-Personal verstanden.

IT-Sicherheitsbeauftragter

Ist gleich der zentrale IT-Sicherheitsbeauftragte gemäß §§ 4 Abs.1, 6 Abs.2 IT-SO. Der IT-Sicherheitsbeauftragte ist zuständig für alle IT-Sicherheitsfragen, die Erstellung einer IT-Sicherheitsrichtlinie, wirkt mit im IT-Sicherheitsprozess und führt den Vorsitz in dem Sicherheitsmanagement-Team. Außerdem koordiniert er die Erstellung von weiteren Konzepten zur IT-Sicherheit.

IT-Sicherheitsrichtlinie

Ist eine systematische Bestandsaufnahme und Analyse der Anforderungen und Maßnahmenplanung für den Bereich der IT-Sicherheit der 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.

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: Personalverwaltung, PICA in den Bibliotheken der Universität.

Key-User

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

LAN

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

Mengengerüst

Angaben über die Mengen aller in dem betreffenden Zusammenhang interessierenden Ressourcen

Netzknoten

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

Netzwerksegmente

Logisch oder physisch getrennte Teile eines Netzwerkes

Passwort

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

Risiko

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

Rolle

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

Schützenswerte Daten

Daten, deren Verlust, Bekanntwerden oder Verfälschung einen erheblichen materiellen und immateriellen Schaden bedeutet (siehe Kapitel 4 Feststellung des Schutzbedarfs)

Sicherheitsmanagement-Team (SMT)

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

Server

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

Transparenz

ist gewährleistet, wenn das IT-Verfahren für die jeweils Sachkundigen in zumutbarer Zeit mit zumutbarem Aufwand nachvollziehbar ist.

Verfahrensverantwortlicher

Trägt die Verantwortung für den Betrieb aller IT-Systeme und für die Datenverarbeitung innerhalb eines Verfahrens.

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, Webseiten oder Datenträger auf den Arbeitsplatzrechner geladen, die bei Ausführung leichten bis schweren Schaden hervorrufen können

Virenscanner

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

Zugriffsrecht

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

Zuständige Stelle

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

Zweckbindung

Personenbezogene Daten dürfen nur für den Zweck verwendet werden, zu dem sie erhoben wurden.

8. Verzeichnis der Rollen für IT-Verfahren und aus organisatorischer und strategischer Sicht

Rolle	Funktion	Querverweis
Präsidium	Höchste Entscheidungsinstanz der Goethe-Universität Frankfurt in allen IT-Fragen Strategische und operative Führung des IT-Einsatzes (Einrichtung des Präsidiums)	Abschnitt 2.3, verschiedene Grundschutzmaßnahmen
IT-Dienstleister	Bereitstellung von zentralen IT-Services für die Goethe-Universität Frankfurt	Abschnitt 2.3, verschiedene Grundschutzmaßnahmen
Für Technik zuständige Abteilung	gewährleistet die Nutzbarkeit und Sicherheit der Gebäude und Räume sowie die Funktionsfähigkeit der betriebstechnischen Anlagen	Abschnitt 3.2.4 und 3.2.5, verschiedene Grundschutzmaßnahmen
Bereichsleitung	Verantwortung für den laufenden IT-Einsatz im jeweiligen Aufgabenbereich sowie für alle bereichsinternen IT-Planungen.	Abschnitt 2.3, verschiedene Grundschutzmaßnahmen
IT-Beauftragter	Ansprechpartner in allen IT-Fragen des Bereichs; Koordination des IT-Einsatzes und der IT-Planung des jeweiligen Bereichs	Abschnitt 2.3, verschiedene Grundschutzmaßnahmen
Verfahrensverantwortlicher	Organisiert und verantwortet die Einführung und den laufenden Betrieb eines IT-Verfahrens einschließlich aller Komponenten und Schnittstellen	Abschnitt 2.2.2 und 2.3, verschiedene Grundschutzmaßnahmen
IT-Personal	Administriert, betreut oder wartet IT-Systeme	verschiedene Grundschutzmaßnahmen
Systemadministrator	Konfiguriert und betreibt IT-Systeme; verantwortlich für den ordnungsgemäßen Betrieb der IT-Systeme	Abschnitt 2.2.2, verschiedene Grundschutzmaßnahmen
Applikationsbetreuer	Parametrisiert und konfiguriert die Anwendungssoftware; Verwaltung von Benutzerrechten; Patchmanagement	Abschnitt 2.2.2
Anwenderbetreuer	I.d.R. zuständig für die Installation und Wartung von Endgeräten und Anwendungssoftware	Abschnitt 2.2.2
Key-User	Weitergabe besonders guter Anwendungskenntnisse an Anwender (Multiplikator-Funktion); erste Ansprechstelle für Anwender	Abschnitt 2.2.2
Anwender	Nutzung von IT-Ressourcen der Goethe-Universität Frankfurt	Abschnitt 2.2.2
Behördlicher Datenschutzbeauftragter	Unterstützung der Universitätsleitung in allen Fragen der Verarbeitung personenbezogener Daten und die Überwachung der ordnungsgemäßen Anwendung von personenbezogenen Daten verarbeitender Systeme	Abschnitt 2.3, verschiedene Grundschutzmaßnahmen

Rolle	Funktion	Querverweis
IT-Sicherheitsbeauftragter	Koordination und Organisation der Informationssicherheit	Abschnitt 2.3
Sicherheitsmanagement-Team	Bestimmen der IT-Sicherheitsziele und -strategien; Fortschreibung der IT-Sicherheitsrichtlinie; Mitwirkung bei der Steuerung des IT-Sicherheitsprozesses	Abschnitt 2.3
Personalvertretung	Achtet auf die Einhaltung der relevanten gesetzlichen Bestimmungen; Vertretung in Gremien der Universität; schließt Dienstvereinbarungen zum IT-Betrieb ab; ist beteiligt an der Genehmigung von IT-Verfahren	Abschnitt 6.1

9. Literaturverzeichnis

9.1 Dokumente der Goethe-Universität Frankfurt

- IT- Sicherheitsordnung der Goethe-Universität vom 07.Mai 2013 (UniReport 14. Mai 2013)

- Allgemeine Nutzungsordnung für die Informationsverarbeitungs-und Kommunikations-Infrastruktur der Johann Wolfgang Goethe-Universität (Allgemeine IuK-Nutzungsordnung) vom 11.September 2008 (UniReport 23.September 2008)

- Satzung der Johann Wolfgang Goethe-Universität zum Studienausweis als Chipkarte vom 6. September 2006 (Chipkarten-Satzung) in der Fassung vom 11. September 2008 (UniReport 23. September 2008)

- Satzung der Johann Wolfgang Goethe-Universität über die Einführung der Universitätskarte „Goethe-Cardplus“ vom 31. März 2009 -Satzung Goethe-Cardplus (UniReport 03.April 2009)

Weitere Regelungen werden auf der Seite der Universität (http://www.satzung.uni-frankfurt.de) veröffentlicht

9.2 IT-Dienstvereinbarungen

DV über den Einsatz von Mobiltelefonen
DV über die gleitende Arbeitszeit an der JWGU
DV Arbeitszeit Universitätsbibliothek
DV Videoüberwachung
DV Universitätskarte
DV über die Einführung und den Betrieb von SAP R/3
DV Schließsysteme
DV zur alternierenden Telearbeit an der JWGU

Derzeit gültige Dienstvereinbarungen sind unter

www.uni-frankfurt.de/47115189/dienstvereinbarungen

nachzulesen

9.3 Externe Dokumente

[Grundschutz-Kataloge]
IT-Grundschutz-Kataloge in der jeweils aktuellen Version

[BSI-Standards zur IT-Sicherheit]
IT-Sicherheitsmanagement und IT-Grundschutz in der jeweils aktuellen Version