Verkündungsblatt

der Fachhochschule Erfurt

Nummer 76

Wintersemester 2019/20

Aus dem Inhalt

IT-Sicherheitsrichtlinie für die Fachhochschule Erfurt 465

Impressum 517

IT-Sicherheitsrichtlinie für die Fachhochschule Erfurt

Version 1.0

15.10.2019

Zuletzt geändert am 15.10.2019

Inhalt

Präambel ... 3
1 Geltungsbereich ... 3
2 Ausgangssituation ... 3
2.1 Grundbegriffe der IT-Sicherheitsrichtlinie ... 4
2.2 IT-Verfahren, Geschäftsprozesse und Verarbeitungstätigkeiten ... 4
2.3 Rollen ... 5
2.4 Verantwortlichkeiten und Organisation der IT-Sicherheit ... 7
3 IT-Grundschutz ... 9
3.1 Definition des Grundschutzes ... 9
3.2 Maßnahmen des IT-Grundschutzes ... 10
3.2.1 Allgemein ... 10
3.2.2 Organisation von IT ... 10
3.2.3 Personal ... 13
3.2.4 Sicherung der Infrastruktur ... 15
3.2.5 Hard- und Softwareeinsatz ... 18
3.2.6 Einsatz von mobilen Geräten ... 20
3.2.7 Zugriffsschutz ... 22
3.2.8 Protokollierung ... 25
3.2.9 System- und Netzwerkmanagement ... 26
3.2.10 Datensicherung ... 28
3.2.11 Datenträgerkontrolle ... 28
4. Feststellung des Schutzbedarfes ... 30
4.1 Schutzbedarfsanalyse ... 31
4.1.1 Vorgehensweise ... 31
4.1.2 Bewertungstabellen ... 33
5 Risikoanalyse ... 37
5.1 Ziel der Risikoanalyse ... 37
5.2 Definition Risiko ... 38
5.3 Vorgehensweise ... 38
5.4 Beispiel ... 39
6 Umsetzung der IT-Sicherheitsrichtlinie ... 44
6.1 Inkraftsetzung und Aktualisierung der IT-Sicherheitsrichtlinie ... 44
6.2 Information über die IT-Sicherheitsrichtlinie ... 45
6.3 Konfliktlösung bei der Umsetzung der IT-Sicherheitsrichtlinie ... 45
6.4 Leitlinienfunktion für andere Dokumente ... 45
7 Glossar ... 46

Präambel

Um das Ziel „ausreichende und angemessene IT-Sicherheit“ an der Fachhochschule Erfurt (FHE) zu erreichen, werden die Empfehlungen und Vorschläge des Bundesamts für Sicherheit in der Informationstechnik (BSI) zugrunde gelegt.

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

1 Geltungsbereich

Die in dieser IT-Sicherheitsrichtlinie beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind für Mitglieder und Bereiche (Dezernate, Fakultäten, Einrichtungen) der FHE verbindlich. Die IT-Sicherheitsrichtlinie gilt darüber hinaus auch für alle externen Nutzer der IT-Infrastruktur der FHE.

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

2 Ausgangssituation

Die FHE setzt in hohem Maße Informationstechnologie in ihren Kernprozessen ein:

- Verwaltung von Personal-, Studierenden- und Prüfungsdaten, Finanzsteuerung u.a.
- Lehre: e-Learning, elektronische Bibliothekssysteme oder das elektronische Management von Lehrveranstaltungen u.a.
- Forschung: Forschungsdatenmanagement, weltweite Kommunikation und Zusammenarbeit, elektronische Publikation und Recherche u.a.

Verbunden mit dem steigenden IT-Einsatz an der FHE steigt auch die Abhängigkeit der Fachhochschule vom Funktionieren der IT. Der zuverlässige IT-Einsatz ist notwendig auf Grund von:

- gesetzlichen Anforderungen, wie Datenschutz, Haushaltsrecht und Steuerrecht
- vertraglichen Anforderungen, wie die Nutzung des DFN-Netzes und die Revisionspflicht gegenüber Drittmittelgebern

Es sind daher Maßnahmen zu treffen, die die Funktionsfähigkeit der FHE 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 FHE 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.

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 FHE enthaltenen zentralen Begriffe erläutert.

Die Beschreibung des Umgangs mit der an der FHE 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 Grundschutz bildet das Fundament der IT-Sicherheit der FHE. Die zur Erreichung des Grundschutzes erforderlichen Maßnahmen werden unabhängig von den einzelnen Verfahren beschrieben. Für IT-Verfahren mit höherem Schutzbedarf müssen über diese Grundschutzmaßnahmen hinaus zusätzliche verfahrensbezogene Maßnahmen erarbeitet werden.

Aufgrund des stetigen Fortschritts auf dem Gebiet der Informationstechnik muss die IT-Sicherheitsrichtlinie regelmäßig überprüft und neuen Anforderungen angepasst werden.

2.1 Grundbegriffe der IT-Sicherheitsrichtlinie

Im Folgenden werden die zentralen Begriffe der IT-Sicherheitsrichtlinie der FHE erläutert.

- **Verfügbarkeit** bezieht sich auf Daten und Verfahren und bedeutet, dass sie zeitgerecht zur Verfügung stehen.
- **Vertraulichkeit** ist gewährleistet, wenn nur Personen, die dazu berechtigt sind, von schützenswerten Daten Kenntnis nehmen können.
- **Integrität** gewährleistet, wenn schützenswerte Daten unversehrt und vollständig bleiben.
- **Authentizität** bedeutet, dass Daten jederzeit ihrem Ursprung zugeordnet werden können.
- **Revisionsfähigkeit** bezieht sich auf die Organisation des Verfahrens. Sie ist gewährleistet, wenn Änderungen an Daten nachvollzogen werden können.

2.2 IT-Verfahren, Geschäftsprozesse und Verarbeitungstätigkeiten

Ein IT-Verfahren (IT-Verbund) besteht aus einem oder mehreren IT-gestützten Geschäftsprozessen, die eine arbeitsorganisatorisch abgeschlossene Einheit mit einem gemeinsamen Ziel bilden. Geschäftsprozesse können sich aus einer oder mehreren Verarbeitungstätigkeiten zusammensetzen. Die Summe aller IT-Verfahren soll den gesamten IT-Einsatz an der FHE lückenlos abbilden.

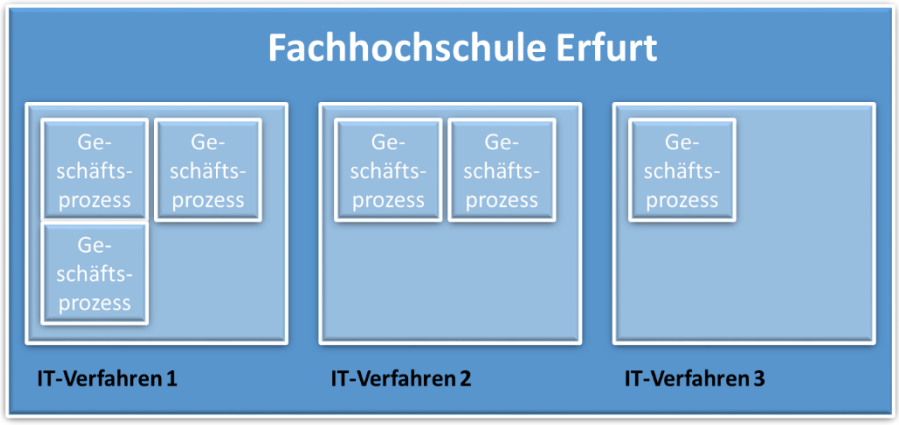

Abbildung 1:

Der gesamte IT-Einsatz der FH soll lückenlos durch IT-Verfahren dokumentiert werden. In dem skizzierten Beispiel sind drei IT-Verfahren dargestellt, die jeweils aus einer unterschiedlichen Anzahl von Geschäftsprozessen bestehen

Abbildung 2:

Geschäftsprozesse setzen sich aus einer oder mehreren Verarbeitungstätigkeiten zusammen

Für jedes IT-Verfahren ist eine Schutzbedarfsanalyse durchzuführen. Dabei ist folgendes zu dokumentieren:

1. Beschreibung der Rollen; ggf. in Form eines Berechtigungskonzepts
2. Angaben über die Anzahl und Art von technischen Einrichtungen und Geräten (Mengengerüst)
3. Angaben der Schnittstellen zu anderen IT-Verfahren, IT-Systemen und sonstigen Diensten
4. Angaben über die vom IT-Verfahren betroffenen Organisationseinheiten
5. Aufstellungsort von Anlagen und Geräten, die wesentliche Funktionen innerhalb des Arbeitsprozesses bzw. IT-Verfahrens erfüllen
6. Zeitplan für die Einführung des Verfahrens sowie ggf. für die Erstellung eines Betreuungskonzepts
7. Betriebshandbuch mit allen für den Betrieb notwendigen Angaben über die im IT-Verfahren erfassten technischen Systeme

2.3. Rollen

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.

Rolle	Funktion	Notwendigkeit
Verfahrensverantwortlicher	• organisiert die Einführung und Betrieb • 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 • verantwortlich für den ordnungsgemäßen Betrieb der IT-Systeme • zuständig für Erstellung eines Betriebs- und Datensicherungskonzepts • zuständig für die Einhaltung des eines Betriebs- und Datensicherungskonzepts	in der Regel immer vorhanden
Applikationsbetreuer	• Parametrisierung und Konfiguration der Anwendungssoftware • Verwaltung von festgelegten Benutzerrechten • administrative Betreuung aus fachlicher Sicht neben und ergänzend zur Systemadministration	in der Regel immer vorhanden

Die konkrete personelle Zuordnung einer Rolle ist abhängig von dem betreffenden IT-Verfahren bzw. IT-Geschäftsprozess. Bei großen und komplexen IT-Geschäftsprozessen kann 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 Applikationsbetreuers 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 konkretem 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.

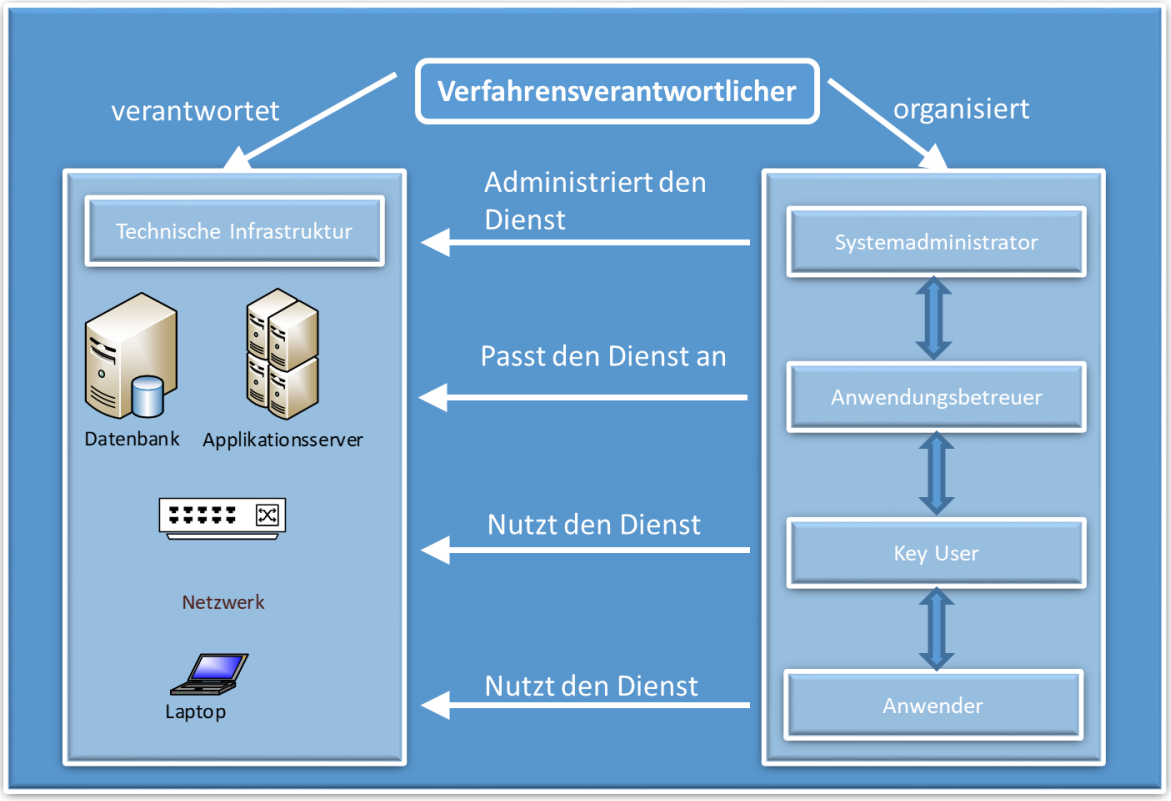

Abbildung 3:Rolle Verfahrensverantwortlicher

2.4 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 FHE auswirken. Die Gewährleistung der IT-Sicherheit erfordert über die Einhaltung der in dieser IT-Sicherheitsrichtlinie aufgestellten Regeln hinaus die aktive Mitarbeit aller beteiligten Personen – und zwar hierarchie- und bereichsübergreifend.

Die für die IT-Sicherheit aus organisatorischer und strategischer Sicht bedeutendsten Rollen sind:

- **Höchste Entscheidungsinstanz (Präsidium)**
  Die höchste Entscheidungsinstanz an der Fachhochschule Erfurt in allen IT-Fragen ist das Präsidium bzw. der Präsident der Fachhochschule Erfurt.
- **Strategische und operative Führung des IT-Einsatzes (CIO)**
  Der Chief Information Officer (CIO) ist für alle Aufgaben der strategischen Führung der Informationstechnologie und der bereichsübergreifenden operativen Vorgaben in enger Abstimmung mit dem Präsidium verantwortlich.
- **Bereitstellung von zentralen IT-Diensten (Zentraler IT-Dienstleister)**
  Der zentrale IT-Dienstleister (Hochschulrechenzentrum der FHE) plant, realisiert, betreibt und gestaltet IT-Infrastrukturen und -Services für die Einrichtungen der FHE. Er bezieht dabei unter anderem Leitungen aus dem IT-DLZ der Thüringer Hochschulen.
- **Koordination und Organisation der Informationssicherheit (IT-Sicherheitsbeauftragter)**

Die Aufgabe der Koordination und Organisation der Informationssicherheit obliegt dem IT-Sicherheitsbeauftragten. Er ist zuständig für die Wahrnehmung aller Belange der Informationssicherheit innerhalb der Fachhochschule Erfurt. Zu den Aufgaben des IT-Sicherheitsbeauftragten gehören u.a.:

  - Den Sicherheitsprozess zu steuern und bei allen damit zusammenhängenden Aufgaben mitzuwirken,
  - die Leitungsebene bei der Erstellung der IT-Sicherheitsrichtlinie zu unterstützen,
  - die Erstellung der IT-Sicherheitsrichtlinie und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren.
- **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)**
  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 der AG IT-Sicherheit über den Status Quo der IT-Sicherheit zu berichten
  - Koordination von sicherheitsrelevanten Projekten
  - Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen
- **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. Er trägt er die Verantwortung für die Einhaltung der Informationssicherheit
- **AG IT-Sicherheit**
  Zu den zentralen Aufgaben der AG IT-Sicherheit gehören:
  - IT-Sicherheitsziele und -strategien zu bestimmen sowie die IT-Sicherheits-richtlinie zu entwickeln,
  - den IT-Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
  - zu überprüfen, ob die in der IT-Sicherheitsrichtlinie geplanten IT-Sicherheitsmaßnahmen wie beabsichtigt funktionieren, also geeignet und wirksam sind,
  - bei der Fortschreibung der IT-Sicherheitsrichtlinie mitzuwirken,
  - die Schulungs- und Sensibilisierungsprogramme für IT-Sicherheit zu konzipieren sowie
  - die Leitungsebene in IT-Sicherheitsfragen zu informieren und zu beraten.

Die Zusammensetzung der Arbeitsgruppe IT-Sicherheit soll möglichst die Vielfalt der unterschiedlichen Anforderungen der Organisationseinheiten (Forschung und Lehre, Dienstleister, Verwaltung) an den IT-Einsatz berücksichtigen.

3 IT-Grundschutz

Die Sicherheit in der Informationstechnik dient der Sicherstellung von Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität und Revisionsfähigkeit von Daten und IT-Anwendungen. Bei der Verarbeitung personenbezogener Daten sind darüber hinaus die auf den Schutzbedarf der Betroffenen ausgerichteten Gewährleistungsziele des Datenschutzes zu beachten, die sich in den Prinzipien der Datenvermeidung, Datensparsamkeit und Erforderlichkeit, sowie der Zweckbindung und Intervenierbarkeit widerspiegeln. Diese Ziele im Zusammenhang und teilweise Abwägung zueinander 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 Fachhochschule Erfurt. 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.

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 Fachhochschule Erfurt in geeigneter Weise bekannt zu geben.

Als Basis für die hier dargestellten IT-Grundschutzmaßnahmen dienen die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die dort beschriebenen Maßnahmen wurden den Besonderheiten der Fachhochschule Erfurt 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 FH Erfurt auf ganze Klassen von Programmen. Das bedeutet, dass viele der in dieser Richtlinie dargestellten Maßnahmen allgemeiner gefasst sind.

Mit dem Begriff „IT-Personal“ werden im Folgenden alle Personen verstanden, die mit der Administration, Wartung und Betreuung von IT-Ressourcen betraut sind. In der Regel handelt es sich um HRZ und Bereichsadministratoren, aber auch andere Beschäftigte der FH Erfurt.

3.2 Maßnahmen des IT-Grundschutzes

3.2.1 Allgemein

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

Verantwortlich für die Initiierung:	CIO
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 FH Erfurt geltenden Regelungen zu richten.

- **Gesamtverantwortung (M2)**

Verantwortlich für Initiierung:	CIO
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 Fakultäten, Instituten, zentralen Bereichen und der Hochschulverwaltung entsprechend den Regelungen des Thüringer Hochschulgesetzes.

3.2.2 Organisation von IT

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

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

Der gesamte IT-Einsatz ist in IT-Verarbeitungstätigkeiten zu gruppieren und zu beschreiben.

- **Rollentrennung (M4)**

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

Für jede IT-Verarbeitungstätigkeit 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 Schnittstellen der verschiedenen Anwenderrollen müssen klar definiert sein. Bei der Rollenbesetzung muss beachtet werden, dass bestimmte Rollen von verschiedenen Personen wahrgenommen werden müssen. Beispielsweise dürfen die Rollen in einem Finanzsystem „sachliche Freigabe“ und „Anordnungsbefugnis“ (Kontrollfunktion vor der Auszahlung) nicht von ein und derselben Person wahrgenommen werden. Auch darf im Campus-Management-System die Eintragung von Prüfungsergebnissen nicht von betroffenen studentischen Mitarbeitern durchgeführt werden.

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

Verantwortlich für Initiierung:	CIO
Verantwortlich für Umsetzung:	Bereichsleitung

Den IT-Beauftragten der Organisationseinheiten kommt im Rahmen des IT-Einsatzes an der FH Erfurt eine zentrale Bedeutung zu, denn sie haben in ihrem Zuständigkeitsbereich die für den IT-Einsatz

gebotenen technischen und organisatorischen Maßnahmen zur IT-Sicherheit zu initiieren und zu koordinieren; sie führen die notwendigen Aufzeichnungen für die Organisationseinheit ihrer Zuständigkeit. Bei Fragen des IT-Einsatzes sind sie sowohl Ansprechpartner für die Mitarbeiter ihrer Organisationseinheit als auch für Dritte (außerhalb ihrer Organisationseinheit). (Siehe Abschnitt 2.3 Verantwortlichkeiten und Organisation der IT-Sicherheit)

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

Verantwortlich für Initiierung:	CIO, Bereichsleitung
Verantwortlich für Umsetzung:	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 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 durch die IT-Organisationsrichtlinie 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 Fehlern (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. Bei einem Sicherheitsvorfall muss der Leiter des HRZ oder IT-Sicherheitsbeauftragte informiert werden. Als Sicherheitsvorfall wird ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit oder Integrität der Informationen, Geschäftsprozesse, IT-Dienste und -Anwendungen der Fachhochschule Erfurt mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für die Fachhochschule Erfurt oder deren Partner entstehen kann. Alle Sicherheitsvorfälle müssen dokumentiert werden.

Ereignisse, die eine Verletzung des Schutzes personenbezogener Daten bedeuten können, sind unverzüglich dem Verfahrensverantwortlichen und dem behördlichen Datenschutzbeauftragten zu

melden, unabhängig davon, ob es sich um einen IT-Sicherheitsvorfall im oben beschriebenen Sinne handelt.

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 Fachhochschule Erfurt betriebenen IT-Verfahren. Es sind eindeutige Zuweisungen der Verantwortlichkeit für die IT-Sicherheit zu schaffen und entsprechende Kontrollmöglichkeiten vorzusehen.

- **Standards für technische Ausstattung (M10)**

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

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

- **Zentralisierung wichtiger Serviceleistungen (M11)**

Verantwortlich für Initiierung:	CIO, Bereichsleitung
Verantwortlich für Umsetzung:	HRZ, IT-Beauftragter, IT-Personal

Eine Reihe von Diensten wird zentral für die Fachhochschule Erfurt 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.). 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.

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

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

Grundsätzlich sind Services, die vom HRZ der Fachhochschule Erfurt bereitgestellt werden, selbst betriebenen Diensten vorzuziehen. Nur wenn der benötigte Dienst nicht vom HRZ der FH Erfurt bereitgestellt wird oder der bereitgestellte Dienst den Anforderungen nicht genügt, dürfen der Dienst und die notwendigen IT-Systeme selbst eingerichtet und betrieben werden.

Die notwendige netzwerktechnische Freischaltung von IT-Systemen, die von Netzen außerhalb der Netze der Fachhochschule Erfurt erreichbar sein sollen, muss über das CIO bei der zuständigen Stelle des HRZ beantragt werden. Der Antrag muss begründet sein.

Zugänge, die zur Wahrnehmung administrativer oder betreuender Aufgaben benötigt werden, sind direkt bei der zuständigen Stelle des HRZ unter Angabe der Gründe zu beantragen.

- **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. (Zum Beispiel wäre es sinnvoll, nur Anbieter mit Zertifikaten des BSI in Betracht zu ziehen.)

- **Allgemeine Notfallvorsorge (M14)**

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

Bei der Einführung neuer IT-Verfahren bzw. neuer IT-Arbeitsprozesse werden im Rahmen der Dokumentationspflichten Analysen zur Ermittlung des Schutzbedarfs und ggf. zur Identifizierung und Begegnung spezifischer Risiken vorgenommen. Basierend auf den Ergebnissen dieser Analysen ist ein Notfallplan zu erstellen, in dem festgelegt wird, wie auf Notfallsituationen adäquat reagiert wird. „Notfall“ bezeichnet eine Situation, in der durch eine Betriebsstörung die Sicherheit der IT und der Schutz der Daten nicht mehr gegeben ist und ein verhältnismäßig hoher Schaden entstehen kann. In einem Notfallplan müssen unter anderem Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten und zum Einsatz von Ausweichmöglichkeiten enthalten sein. Im Falle einer Datenschutzverletzung schließt dies auch Maßnahmen zur Wiederherstellung des Schutzes personenbezogener Daten, zur Verhinderung ihrer weiteren Verbreitung und gegebenenfalls zur Abmilderung der möglichen nachteiligen Auswirkungen ein. Mindestanforderung ist ein Alarmierungsplan, 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 und Datenschutzvorfälle unverzüglich den jeweils Zuständigen (Verfahrensverantwortlicher, Datenschutzbeauftragter) 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, CIO

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 Fachhochschule Erfurt 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. Das Ziel dabei muss sein, dass alle Aktivitäten auf eine konkrete Person zurückführbar sind. Beispielsweise sollten anstelle eines generischen Administrator-Accounts einzelne, personenbezogene Accounts mit den erforderlichen Berechtigungen vergeben werden. Die technischen Voraussetzungen für die Wahrnehmung einer Vertretung sollten möglichst ständig eingerichtet sein.

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

- **Qualifizierung (M18)**

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

IT-Personal darf erst nach ausreichender Schulung mit IT-Verfahren arbeiten. Dabei sind ihnen die für sie geltenden Sicherheitsmaßnahmen, die rechtlichen Rahmenbedingungen sowie ggf. die Erfordernisse des Datenschutzes zu erläutern. Es muss sichergestellt sein, dass 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:	CIO, Bereichsleitung
Verantwortlich für Umsetzung:	Technische Abteilung, Bereichsleitung, IT-Beauftragter

Die vollständige Zugangskontrolle zu allen Räumen, in denen Geräte mit zentraler Bedeutung für die Netzinfrastruktur der Fachhochschule Erfurt 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:	DBL, 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 und unter Aufsicht erfolgen.

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

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-Personal

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
Verantwortlich für Umsetzung:	IT-Personal

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, DBL

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, sollten nach Möglichkeit protokolliert werden. Es sei noch einmal auf die Maßnahme M9 verwiesen.

- **Stromversorgung und Überspannungsschutz (M26)**

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

Alle wichtigen IT-Systeme dürfen nur an eine ausreichend dimensionierte und gegen Überspannungen abgesicherte Stromversorgung angeschlossen werden. Eine entsprechende Versorgung ist herzustellen. Bei Einsatz von Geräten mit redundant ausgelegter Stromversorgung muss 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 DBL zur Verfügung zu stellen. Alle Arbeiten an der Stromversorgung müssen mit dem IT-Beauftragten abgestimmt werden.

- **USV (M27)**

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

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

- **Brandschutz (M28)**

Verantwortlich für Initiierung:	IT-Beauftragter, DBL, Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	DBL

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.

- **Schutz vor Wasserschäden (M29)**

Verantwortlich für Initiierung:	IT-Beauftragter, DBL, Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	DBL

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, DBL, Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	DBL

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:	Verfahrensverantwortlicher
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:	Verfahrensverantwortlicher
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-Sicherheits- und ggf. Datenschutzaspekte 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.

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

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

Die Entwicklung großer, komplexer Systeme, für die auf Grund ihrer Größenordnung die Regeln des IT-Projektleitfadens gelten, müssen nach den Regeln anerkannter Vorgehensmodelle zur Softwareentwicklung durchgeführt werden. (V-Modell, Scrum)

- **Kontrollierter Softwareeinsatz (M35)**

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

Auf Rechnersystemen, die IT-Ressourcen der FH-Erfurt nutzen, darf zum Zweck des Schutzes von hochschuleigener Hardware und dem Hochschulnetz nur Software installiert werden, die vom HRZ 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 (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
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 Arbeitsplatz-PCs ist, soweit möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Regelmäßig sind die Virenerkennungsmuster automatisiert 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 Rechner-Konfiguration (M39)**

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

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

- **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. müssen gesondert dokumentiert werden. Siehe dazu auch Abschnitt 2.2.1 Erfassung und Dokumentation von IT-Verarbeitungstätigkeiten.

- **Ausfallsicherheit (M41)**

Verantwortlich für Initiierung:	IT-Beauftragter (bereichsspezifisch)
	Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	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 Reaktionszeiten hinreichend verfügbar gehalten werden.

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

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

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. Die Speicherung von besonderen Kategorien personenbezogener Daten nach Artikel 9 DSGVO in der Cloud ist nicht gestattet. Für personenbezogene Daten gelten die Regelungen zur Auftragsdatenverarbeitung des Thüringer 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 Fachhochschule Erfurt bei der Nutzung des mobilen Geräts.

- **Schutz vor unbefugten 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. 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 (zum Beispiel 1 Minute) 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 sofort 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.

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

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

Schützenswerte Daten dürfen auf mobilen Geräten nur verschlüsselt 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 Gerät abgelegt werden.

3.2.7 Zugriffsschutz

Grundsätzlich gilt, dass nur die Personen Zugang zu dem Netz und den damit verfügbaren Ressourcen der Fachhochschule Erfurt 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 stets nachvollziehbar ist, wer wann wie lange die anonyme Kennung benutzt hat.

- **Bereitstellung von Verschlüsselungssystemen (M50)**

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

Zur Absicherung besonders schützenswerter Daten, insbesondere auf mobilen Geräten, müssen geeignete Systeme (Programme oder spezielle Hardware) zur Verschlüsselung durch das HRZ der Fachhochschule Erfurt bereitgestellt werden.

- **Netzzugänge (M51)**

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

Der Anschluss von Systemen über die Netzzugänge der Fachhochschule Erfurt hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Access Points o.ä.) ohne Absprache mit dem IT-Beauftragten der Organisationseinheit und ggf. mit dem Datenschutzbeauftragten ist unzulässig.

- **Ausscheiden von Mitarbeitern (M52)**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	DPR, Bereichsleitung

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 über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung des ausscheidenden Mitarbeiters zugeordnet sind. Vor dem Ausscheiden sind sämtliche Unterlagen, die sicherheitsrelevante Angaben enthalten sowie ausgehändigte Schlüssel 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, wie beispielsweise für Systemadministratoren. 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 persönliche Administratorkennung. Für Arbeiten, die keine besonderen Berechtigungsprivilegien erfordern, sind Standard-Benutzerkennungen zu verwenden.

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

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

Das HRZ der Fachhochschule Erfurt hat 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, 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. Idealerweise sollte das Passwort nicht notiert werden. Für die Wahl von Passwörtern gelten folgende Regeln:

- 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 besteht aus mindestens 8 aber höchstens 12 verschiedenen Zeichen
- Es dürfen maximal 2 gleiche Zeichen aufeinander folgen
- Es muss mindestens ein nummerisches Zeichen enthalten
- Umlaute, $.?,`, ´ und # sind verboten

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 Fachhochschule Erfurt benutzt werden, dürfen nicht für andere Zwecke verwendet oder auf externen 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 Kompromittierung des Systems besteht. Auch wenn Passwörter versehentlich bei anderen Systemen oder anderen Anbietern von Diensten eingegeben werden, muss das Passwort gewechselt werden. Bei der Abgabe von Rechnern oder Speichermedien, auf denen Passwörter abgelegt sind, müssen dann die betreffenden Passwörter gewechselt werden, wenn eine vorherige Löschung der Passwörter nicht gewährleistet werden kann (z.B. bei Abgabe eines Rechners im Reparaturfall).

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.

Für die Erstanmeldung neuer Benutzer müssen Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen.

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 sollten Passwörter nicht unverschlüsselt übertragen werden.

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.

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

Es ist zu prüfen, inwieweit die Zugriffserlaubnis 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, 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:	CIO
Verantwortlich für Umsetzung:	IT-Personal, Anwender

Für dienstliche Belange muss die dienstliche E-Mail-Adresse der Fachhochschule Erfurt 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 Fachhochschule Erfurt 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 sichergestellt sein, dass nur die Personen Zugriff auf die Protokolle erlangen können, bei denen die Protokollauswertung Bestandteil der dienstlichen Aufgaben ist. Das Prinzip der Zweckbindung gemäß Thüringer 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 Thüringer Datenschutzgesetz zu beachten.

3.2.9 System- und Netzwerkmanagement

Die gesamte elektronische Kommunikation der Fachhochschule Erfurt wird durch eine Sicherheitsinfrastruktur in angemessener Weise geschützt. Besonderes Augenmerk gilt dabei der Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf. Alle Nutzer der Hochschul-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 Fachhochschule Erfurt 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
Verantwortlich für Umsetzung:	IT-Personal

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

Es müssen geeignete Maßnahmen getroffen werden, um Überlastungen und Störungen im Netzwerk frühzeitig zu erkennen und zu lokalisieren. Es muss geregelt und sichergestellt sein, dass auf die für diesen Zweck eingesetzten Werkzeuge nur die dazu befugten Personen zugreifen können. Der Kreis der befugten Personen ist auf das notwendige Maß zu beschränken.

- **Deaktivierung nicht benötigter Netzwerkzugänge (M65)**

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

Es sind alle nicht benötigten Netzwerkzugänge zu deaktivieren, damit ein unbefugter Zugang zum Netz der Fachhochschule Erfurt verhindert wird.

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

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

Die gesamte Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf oder mit externen Partnern darf ausschließlich über kontrollierte Kanäle erfolgen, die durch ein spezielles Schutzsystem geführt werden. Die Installation und der Betrieb anderer Kommunikationsverbindungen neben den Netzverbindungen der Fachhochschule Erfurt sind nicht gestattet. Falls auf Grund besonderer Umstände die Installation anderer Kommunikationswege unumgänglich ist, muss dies zuvor durch die zuständige Stelle genehmigt werden. Jeder Zugriff Externer ist zu protokollieren.

- **Rechnernamen (M67)**

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

Zur Erleichterung der Notfallvorsorge und der Missbrauchsnachverfolgung muss jeder Rechner, der mit den Netzen der Fachhochschule Erfurt verbunden ist, einen DNS- Eintrag (DNS = Domain Name System) der Fachhochschule Erfurt besitzen.

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 Fileserver nicht möglich ist, müssen geeignete Maßnahmen zur Datensicherung selbst ergriffen werden.

- **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 testweise Wiedereinspielen von Datensicherungen muss 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 Unternahmen 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, 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. Die Datenlöschung ist zu protokollieren.

Bei der Vergabe dieser Aufgaben an externe Dienstleister sind neben der gebotenen Sorgfalt bei der Auswahl des Auftragnehmers auch die übrigen Bestimmungen über Auftragsdatenverarbeitung zu beachten.

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, 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.

4. Feststellung des Schutzbedarfes

Die eingesetzte Informationstechnik ist nicht aus sich heraus, sondern vielmehr wegen ihres Wertes für die Anwender bzw. im Falle personenbezogener Daten auch für die Betroffenen 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, 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.

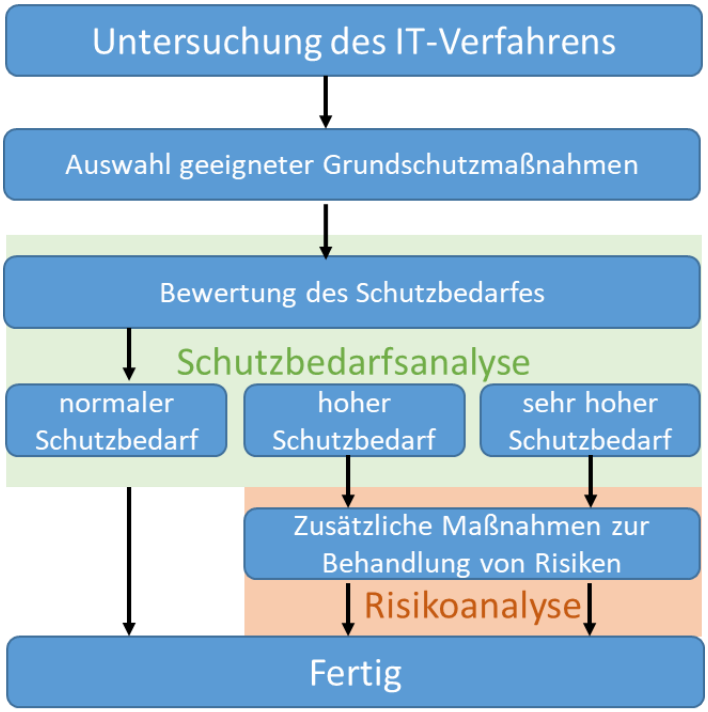

Abbildung 4:

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.

Schritt 1: 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*

Schritt 2: 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*

Schritt 3: 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 Fachhochschule Erfurt 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.

Schritt 4: 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 (Maximum- Prinzip).

Beispiel Vertraulichkeit:

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

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 Bundesamtes für Sicherheit in der Informationstechnik (BSI).

4.1.2.1 Verlust von Vertraulichkeit

Verlust von Vertraulichkeit				
Schadens-kategorien	**Bedrohung**	**Abschätzung des Schadens**		
Beeinträchtigung des inforationellen 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	… 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	... kann für die Betroffenen möglicherweise zu einer gravierenden Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Miss-brauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder
Beeinträchtigung der persönlichen Unversehrtheit	Missbrauch der Daten ...	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen	... 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 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 ist wesentlich	... gefährdet die Aufgabenerfüllung der Fachhochschule Erfurt. Kernprozesse der Hochschule können massiv behindert werden.
Negative Außenwirkung	Missbrauch der Daten ...	…führt höchstens zu geringem Ansehensverlust eines Teilbereichs der FHE bei einer eingeschränkten Öffentlichkeit	... führt zu einem Ansehensverlust der FHE bei einer eingeschränkten Öffentlichkeit oder einem hohen Ansehensverlust eines Teilbereichs der	... führt zu einem Ansehensverlust der FHE 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**

4.1.2.2 Verlust von Integrität

Verlust von Integrität				
Schadens-kategorien	**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	… 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	... 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
Beeinträchtigung der persönlichen Unversehrtheit	Unberechtigte Veränderung der Daten ...	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen	... 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 geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit ist unwesentlich	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit ist	... gefährdet die Aufgabenerfüllung der Fachhochschule Erfurt. Kernprozesse der Hochschule können massiv behindert werden.
Negative Außenwirkung	Unberechtigte Veränderung der Daten ...	…führt höchstens zu geringem Ansehensverlust eines Teilbereichs der FHE bei einer eingeschränkten Öffentlichkeit	... führt zu einem Ansehensverlust der FHE bei einer eingeschränkten Öffentlichkeit oder einem hohen Ansehensverlust eines Teilbereichs der	... führt zu einem Ansehensverlust der FHE 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**

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.

Verlust von Verfügbarkeit				
Schadens-kategorien	**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	… 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	... kann für die Betroffenen möglicherweise zu einer gravierenden Beeinträchtigung des informationellen Selbstbestimmungsrechts führen. Ein möglicher Miss-brauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder
Beeinträchtigung der persönlichen Unversehrtheit	Verlust der Daten ...	... führt zu keiner bis maximal leichter Beeinträchtigung der persönlichen	... 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 geringfügig beeinträchtigen. Einzelne Arbeitsprozesse können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit ist unwesentlich	... würde die Aufgabenerfüllung eines Teilbereichs einer Organisationseinheit erheblich beeinträchtigen. Arbeitsprozesse mit zentraler Bedeutung können behindert werden. Die Aufgabenerfüllung einer Organisationseinheit ist	... gefährdet die Aufgabenerfüllung der Fachhochschule Erfurt. Kernprozesse der Hochschule können massiv behindert werden.
Negative Außenwirkung	Verlust der Daten ...	…führt höchstens zu geringem Ansehensverlust eines Teilbereichs der FU bei einer eingeschränkten Öffentlichkeit	... führt zu einem Ansehensverlust der FHE bei einer eingeschränkten Öffentlichkeit oder einem hohen Ansehensverlust eines Teilbereichs der	... führt zu einem Ansehensverlust der FHE 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**

4.1.2.4 Verstoß 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 Fachhochschule Erfurt eine Rolle spielen könnten:

Datenschutzgesetze,

- Thüringer Datenschutzgesetz (ThürDSG)
- Bundesdatenschutzgesetz (BDSG)
- EU-DSGVO
- Thüringer Hochschul-Datenschutzverordnung

Hochschulgesetze bzw. -verordnungen,

- Thüringer Hochschulgesetz

Vorschriften zur Mitbestimmung

- Rahmendienstvereinbarung **Informations- und Kommunikationstechnik (IuK)**

Verstoß gegen Gesetze, Vorschriften und Verträge			
Bedrohung	**Abschätzung des Schadens**		
Bekannt werden der Daten für Unberechtigte ... Unberechtigte Veränderung der Verlust der Daten	… 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 FHE ruinös sind.
daraus resultierender	**normal**	**hoch**	**sehr hoch**

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 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)

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

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 Objekte wirken

können. Die daraus resultierenden Schäden werden nach der im Kapitel 4 verwendeten dreiteiligen Werteskala (normal, hoch, sehr hoch) klassifiziert. Danach wird abgeschätzt, mit welcher Häufigkeit

ein Schaden in dieser Höhe zu erwarten ist. Am Ende sind die Risiken einer Risikoklasse zuzuordnen.

Untragbare Risiken müssen durch zusätzliche Maßnahmen auf das für die Fachhochschule Erfurt 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 Fachhochschule Erfurt 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

Schritt 3: Bestimmung der Häufigkeit von Schäden Hilfsmittel

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

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	Grundbe-drohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Technisches Versagen	Verfügb.	Produktivsysteme	3	sehr selten	Untragbar	M-01: Wartungsvertrag Produktivsystem
	Verfügb.	Weitere Server	2	sehr selten	Tragbar	M-02: Wartungsvertrag weitere Server
	Verfügb.	Arbeitsplatz-PCs	1	selten	Tragbar	
	Verfügb.	Drucker	1	selten	Tragbar	
	Verfügb.	Zentrale Netzwerkkomponenten	2	selten	Untragbar	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Diebstahl	Verfügb. Vertraul.	Server	2	selten	Untragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude M-14: Zugriffsschutz
Spannungsschwankungen, Blitzschlag	Verfügb.	Produktivsystem	2	sehr selten	Tragbar	M-07: Unterbrechungsfreie Stromversorgung
	Verfügb.	Weitere Server	1	sehr selten	Tragbar	M-07: Unterbrechungsfreie Stromversorgung
Fehlbedienung	Vertraul. Integrit.		1	sehr selten	Tragbar	
Sabotage	Verfügb.	Produktivsystem	1	sehr selten	Tragbar	
	Verfügb.	Weitere Server	1	sehr selten	Tragbar	
Unkontrollierter Zugang	Verfügb. Integrit. Vertraul.	Zentrale Server	2	selten	Untragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude M-14: Zugriffsschutz
	Integrit. Vertraul.	Clients	2	selten	Untragbar	M-08: Zugangsschutz Clients

Objektkategorie:	**Infrastruktur**					
Bezeichnung der Bedrohung	Grundbe-drohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Höhere Gewalt, Terror, Vandalismus	Verfügb.	Serverraum	1	praktisch nie	Tragbar	
	Verfügb.	Zentrale Netzkomponenten	1	sehr selten	Tragbar	
Feuer	Verfügb.	Serverraum	1	sehr selten	Tragbar	
	Verfügb.	Netzkomponenten	1	sehr selten	Tragbar	
Wasser	Verfügb.	Serverraum	1	sehr selten	Tragbar	
	Verfügb.	Netzkomponenten	1	sehr selten	Tragbar	
Überhitzung	Verfügb.	Serverraum	1	öfter	Untragbar	M-09: Klimatisierung
Ausfall der Stromversorgung	Verfügb.	Zentrale Hardware	1	sehr selten	Tragbar	M-07: Unterbrechungsfreie Stromversorgung
Unbefugter Zugang	Vertraul.	Serverraum	2	sehr selten	Tragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude
	Vertraul.	Arbeitsräume	1	selten	Tragbar	M-10: Nicht öffentliche Räume

Objektkategorie:	**Kommunikation**					
Bezeichnung der Bedrohung	Grundbe-drohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Ausfall	Verfügb.	Netzwerk	2	sehr selten	Tragbar	M-05: Wartungsvertrag Netzkomponenten, Redundanz
Überlastung	Verfügb.	Netzwerk	1	selten	Tragbar	
Abhören	Vertraul.	Netzwerk	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung
Manipulation	Vertraul. Integrit.	Netzwerk	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung
Anschließen zusätzlicher Endgeräte	Vertraul. Integrit.	Personenbezogene Daten	2	selten	Untragbar	M-11: Abgeschottetes Netz, Zugangsschutz Netzkomponenten
Unerlaubter Zugang	Vertraul. Integrit.	Netzwerk	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung

Objektkategorie:	**Datenträger**					
Bezeichnung der Bedrohung	Grundbe-drohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Unkontrollierter Zugriff	Verfügb. Integrit. Vertraul.	Sicherungsbänder	2	sehr selten	Tragbar	M-12: Verschlüsselung der Datensicherung, Zugangsschutz
Beschädigung	Verfügb. Integrit.	Sicherungsbänder	1	sehr selten	Tragbar	
	Verfügb. Integrit.	Festplatten	1	sehr selten	Tragbar	M-13: Redundante Speichersysteme, Spiegelplatten
Fehlerhafte Erzeugung	Verfügb. Integrit.	Datenträger	1	sehr selten	Tragbar	
Unzureichende Entsorgung	Vertraul.	Datenträger	2	prak-tisch nie	Tragbar	
Diebstahl	Verfügb. Vertraul.	Datenträger	3	sehr selten	Untragbar	M-12: Verschlüsselung der Datensicherung, Zugangsschutz

Objektkategorie:	**Software, Daten**					
Bezeichnung der Bedrohung	Grundbe-drohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Unerlaubtes Aufspielen von Software	Verfügb.	Software, Daten	1	sehr selten	Tragbar	M-14: Zugriffsschutz Server
Fehlbedienung	Verfügb. Integrit. Vertraul.	Betriebssystem, Datenbank	1	sehr selten	Tragbar	
Unerlaubter Zugriff und Einblick	Integrit. Vertraul.	Datenbank, Daten, Passwörter	2	sehr selten	Tragbar	M-06: Zugangsschutz Serverraum, gesichertes Gebäude M-14: Zugriffsschutz Server
Mangelhafte Verwaltung der Zugriffsrechte	Integrit. Vertraul.	Datenbank	2	selten	Untragbar	M-15: Rollentrennung
Schadprogramme (Computerviren)	Verfügb. Integrit.	Betriebssystem	1	sehr selten	Tragbar	
	Vertraul. Integrit.	Clients	1	öfter	Untragbar	M-16: Virenscanner

Objektkategorie:	**Papier**					
Bezeichnung der Bedrohung	Grundbe-drohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Unvollständigkeit, mangelnde Aktualität	Verfügb.	Systemdokumentation	1	sehr selten	Tragbar	
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Tragbar	
Unzureichende Entsorgung	Vertraul.	Systemdokumentation	1	sehr selten	Tragbar	
	Vertraul.	Personenbezogene Daten	2	selten	Untragbar	M-17: Schredder
Verlust	Verfügb.	Systemdokumentation	1	sehr selten	Trag- bar	

Objektkategorie:	**Personen**					
Bezeichnung der Bedrohung	Grundbe-drohung	Bedrohtes Objekt bzw. Objektgruppe	Schadenshöhe	Häufigkeit	Risikoklasse	Maßnahmen
Ausfall	Verfügb.	Administratoren, Applikationsbetreuer	2	selten	Untragbar	M-18: Vertretung
Unkenntnis	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer	1	sehr selten	Tragbar	
	Integrit. Vertraul.	Anwender	1	sehr selten	Tragbar	
Überlastung	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer	2	sehr selten	Tragbar	M-15: Rollentrennung M-18: Vertretung
	Integrit. Vertraul.	Anwender	1	sehr selten	Tragbar	
Fehlende Kontrollen und Regelungen	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer	2	selten	Untragbar	M-19: Kontrolle der Akteure
	Integrit. Vertraul.	Anwender	2	sehr selten	Tragbar	M-19: Kontrolle der Akteure
Nachlässige Passworthandhabung	Vertraul.	Passwörter	2	sehr selten	Tragbar	M-20: Festlegung der Passwortregeln
Kriminelle Absicht	Verfügb. Integrit. Vertraul.	Administratoren, Applikationsbetreuer, Anwender	2	sehr selten	Tragbar	M-15: Rollentrennung M-21: Kontrolle der Protokoll-Dateien
	Verfügb. Integrit. Vertraul.	Externe	2	sehr selten	Tragbar	M-11: Abgeschottetes Netz, Verschlüsselung M-06: Zugangsschutz M-14: Zugriffsschutz

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

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. Der Vertrag dieser Rechnersysteme sieht eine 4-stündige Reaktionszeit und eine „Next Business 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.

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.

6 Umsetzung der IT-Sicherheitsrichtlinie

6.1. Inkraftsetzung und Aktualisierung der IT-Sicherheitsrichtlinie

Das Präsidium der Fachhochschule Erfurt setzt die IT-Sicherheitsrichtlinie in Kraft.

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

1.	Beauftragung	Das Präsidium der Fachhochschule Erfurt beauftragt die Arbeitsgruppe AG IT-Sicherheit und Datenschutz mit der Pflege und Fortschreibung der IT-Sicherheitsrichtlinie.

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

6.2 Information über die IT-Sicherheitsrichtlinie

Alle Nutzer von IT-Ressourcen der Fachhochschule Erfurt müssen über die für sie relevanten Teile der IT-Sicherheitsrichtlinie informiert werden. Neue Mitglieder der Fachhochschule Erfurt müssen auf die geltende IT-Sicherheitsrichtlinie beim Eintritt in die Fachhochschule hingewiesen werden. Nicht-Mitglieder, die IT-Ressourcen der Fachhochschule Erfurt nutzen, müssen von der beauftragenden oder einladenden FH-Stelle auf die für sie relevanten Teile der IT-Sicherheitsrichtlinie nachweislich hingewiesen werden. Die beauftragende oder einladende FH-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 vorausgesetzt 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 der CIO über den Dissens informiert werden. Der CIO trifft auf Basis der geltenden Richtlinien eine Entscheidung in der strittigen Sache.

Stellt eine Stelle an der Fachhochschule Erfurt 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 den CIO. Der CIO 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

AG IT-Sicherheit

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

Anwender

Endbenutzer von IT-Systemen

Anwenderbetreuung / Hotline

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

Anwendungsbetreuung

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

Applikationsbetreuer

betreut Anwendungssoftware und sorgt für deren ordnungsgemäßen Betrieb

Arbeitsplatzrechner

Endgerät für die Aufgaben des Anwenders

Auftragsdatenverarbeitung

Verarbeitung von Daten im Auftrag durch andere Stellen.

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

Anwenderbetreuer

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

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.

Thüringer Datenschutzgesetz (ThDSG)

Regelungen des Freistaates Thüringen zum Schutz personenbezogener Daten, vgl. auch Bundesdatenschutzgesetz (BDSG)

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.

CIO

Der Chief Information Officer-Gremium (CIO-) wird durch das Präsidium bestimmt und ist für alle Aufgaben der strategischen Führung der Informationstechnologie und der bereichsübergreifenden operativen Vorgaben verantwortlich.

Datenvermeidung

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

Datensparsamkeit

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

Datenschutz

Regelungen und Maßnahmen für die Verarbeitung personenbezogener Daten

Datensicherheit

Sicherstellung von Integrität, Vertraulichkeit und Verfügbarkeit von Daten

Datensicherung

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

Datenträger

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

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), das an ein Daten- oder Telekommunikationsnetzes angeschlossen ist.

Erforderlichkeit

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

Grundschutz

Schreibt allen Nutzern von IT-Ressourcen der Fachhochschule Erfurt einen einheitlichen Katalog von Sicherheitsmaßnahmen im Umgang mit Informationstechnik vor.

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.

Informationelles Selbstbestimmungsrecht

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

IT

Informationstechnik

IT-Arbeitsplatz

Arbeitsplatz an dem die 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-Grundschutz

Grundschutz

IT-Grundschutzhandbuch

Im IT-Grundschutzhandbuch werden Standardsicherheitsmaßnahmen für typische IT-Systeme empfohlen, herausgegeben vom BSI

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

IT-Sicherheitsrichtlinie

ist eine systematische Bestandsaufnahme und Analyse der Anforderungen und Maßnahmenplanung für den Bereich der IT-Sicherheit der Fachhochschule Erfurt. Sie 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 unter Angabe der technischen und organisatorischen Konzepte und Maßnahmen beschrieben. Beispiele für IT-Verfahren: Personalverwaltung, Campusmanagement

Key-User

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

LAN

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

Mengengerüst

Angaben über die Mengen aller in dem betreffenden Zusammenhang interessierenden Ressourcen

Netzknoten

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

Netzwerksegmente

Logisch oder physisch getrennte Teile eines Netzwerkes

Passwort

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

Risiko

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

Rolle

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

Schützenswerte Daten

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

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 Fachhochschule Erfurt unterschiedlich sein können.

Zweckbindung

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

IMPRESSUM

Herausgeber:
Fachhochschule Erfurt,
Rektor der FH Erfurt, Postfach 45 01 55, 99051 Erfurt

Redaktion:
Zentrum für studentische und akademische Angelegenheiten
Victoria Völker, Altonaer Straße 25, 99085 Erfurt
Tel. (0361) 6700-860, E-Mail: victoria.voelker@fh-erfurt.de

Gestaltung:
Doreen Glaser, Altonaer Straße 25, 99085 Erfurt

Das „Verkündungsblatt der FH Erfurt“ ist das in § 3 Absatz 2 des Thüringer Hochschulgesetzes (ThürHG) vom 10. Mai 2018 (GVBl. S. 149 ff), zuletzt geändert durch Artikel 128 des Gesetzes vom 18. Dezember 2018 (GVBl. S. 731) vorgesehene amtliche Verkündungsblatt der Hochschule. Einzelheiten zu Erscheinungsweise, Verbreitung, Bezugsmöglichkeiten und Bezugsbedingungen sind in der „Richtlinie für das Verkündungsblatt der FH Erfurt“ geregelt, auf die hiermit ausdrücklich verwiesen wird.