Freie Universität Berlin

Kommentierte
IT-Grundschutzmaßnahmen für IT-Personal

Auszug aus der IT-Sicherheitsrichtlinie
für die Freie Universität Berlin

August 2009

Inhaltsverzeichnis

1. IT-Grundschutz

1.1. Maßnahmen des IT-Grundschutzes für IT-Personal

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

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

1.1.1. Allgemeines

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

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

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

Kommentar:

Die Maßnahme soll vergegenwärtigen, dass bei der Beschaffung, der Entwicklung und dem Einsatz von Hard- und Software entsprechende Regelungen einzuhalten sind. Dabei spielen vor allem die Beachtung des Datenschutzes sowie der Mitbestimmungsrechte eine zentrale Rolle. Ferner sollte hinsichtlich des IT-Einsatzes das Gebot der Wirtschaftlichkeit beachtet werden. Da die Freie Universität Berlin als öffentliche Stelle des Landes Berlin in der Nachweispflicht gegenüber dem Rechnungshof steht, sollten willkürliche und unbedachte IT-Anschaffungen vermieden werden. Die zentrale Beschaffungsstelle der Freien Universität Berlin beispielsweise ist aufgrund der Vielzahl von Erwerbungen in der Lage, günstige Angebote einzuholen und zu beschaffen.

- **Gesamtverantwortung (M2.2)**

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

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

Kommentar:

Diese Maßnahme zielt in erster Linie darauf ab, deutlich zu machen, wer die Verantwortung auf den verschiedenen Ebenen trägt. Damit soll verhindert werden, dass durch unklare Verantwortlichkeiten schwerwiegende Sicherheitsvorfälle zusätzlich verschärft werden.

1.1.2. Organisation von IT-Sicherheit

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

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

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

Kommentar:

Eine vollständige und korrekte Erfassung der geplanten und vorhandenen IT-Verfahren dient nicht nur der Wartung, Fehlersuche, Instandsetzung und Überprüfung, sondern bildet ebenso die Grundlage für den Mitbestimmungsprozess. Zu beachten ist, dass die in der Maßnahme genannten Bestandteile einer Verfahrensbeschreibung nur einen Ausschnitt darstellen. Eine umfassende Aufzählung der erforderlichen und mit den Personalvertretungen abgestimmten Inhalte ist in der IT-Rahmendienstvereinbarung enthalten.

- **Rollentrennung (M2.4)**

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

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

Kommentar:

Es ist wichtig, die Zuordnung der Rollen eindeutig zu definieren bzw. festzulegen, damit klar ist, wer für was verantwortlich ist. Nur so können Kompetenzstreitigkeiten unmissverständlich geregelt werden und der IT-Sicherheitsprozess kann an der Freien Universität Berlin effizient und effektiv umgesetzt werden.

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

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

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

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

Kommentar:

Gemeinsam mit der Bereichsleitung und den Verfahrensverantwortlichen hat der IT-Verantwortliche u.a. die Aufgabe, herauszufinden, wie schützenswert die verarbeitenden Daten sind. Sobald er festgestellt hat, wie schützenswert die Daten sind, muss er entsprechende Maßnahmen und Regelungen treffen, damit gewährleistet werden kann, dass Vertraulichkeit, Verfügbarkeit und Integrität der Daten gesichert sind. Hierbei ist es besonders wichtig, dass der IT-Verantwortliche dafür sorgt, dass diese Maßnahmen auch umgesetzt werden und dass der Zugrifft auf die Daten klar geregelt ist. Die Etablierung der IT-Verantwortlichen in den einzelnen Bereichen der Freien Universität Berlin ist für den Gesamtsicherheitsprozess zentral.

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

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

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

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

Darüber hinaus sind die Regelungen der bestehenden IT-Grundsatzvereinbarung zur Dokumentation von IT-Verfahren zu beachten. Nur dokumentierte Verfahren dürfen betrieben werden. Der IT-Verantwortliche sorgt für die aktuelle Dokumentation der Verfahren seiner Organisationseinheit. Der IT-Verantwortliche ist verantwortlich für die Erstellung und Pflege der Dokumentation der Verfahren seiner Organisationseinheit. Verfahrensverantwortliche, Systemadministratoren und Applikationsbetreuer sind dabei durch die IT-Organisationsrichtlinie zur Mitarbeit verpflichtet.

Kommentar:

Die Dokumentation ist nicht nur Grundlage für die Aufrechterhaltung der IT-Sicherheit und somit Bedingung für die Weiterentwicklung des IT-Sicherheitsprozesses, sondern dient der Ursachenerkennung und -beseitigung von Störungen. Eine ausführliche Verfahrensdokumentation bildet die Grundlage für Mitbestimmungsprozesse und kann Schwächen in der Einhaltung des Datenschutzes aufzeigen.

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

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

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

Kommentar:

Das Ziel, eine vollständige Dokumentation und somit eine schnelle und effektive Behebung von sicherheitskritischen Vorfällen zu ermöglichen, macht es erforderlich, allen Mitarbeitern bekannt zu geben, wer im Falle von Sicherheitsproblemen zu benachrichtigen ist.

Beispiel: Es ergeben sich Hinweise auf manipulierte Daten, die wichtige Kernprozesse der Freien Universität Berlin betreffen. Werden diese Manipulationen ignoriert und in der Folge nicht entsprechend gehandelt, kann dies unvorhersehbare Schäden nach sich ziehen, wie beispielsweise die fehlerhafte Darstellung von Leistungen der Freien Universität Berlin.

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

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	Verfahrensverantwortlicher

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

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

Kommentar:

Die schriftliche Fixierung vereinbarter Sachverhalte ist zum Zwecke der Vermeidung von Streitfällen aufgrund unpräziser Verabredungen zwischen der Dienststelle und dem externen Auftraggeber von Bedeutung. Die Erfahrung hat gezeigt, dass ein Verzicht dieser Vorgehensweise zu Problemen hinsichtlich des Umfangs und der Gestaltung der Auftragsdatenverarbeitung bis hin zu rechtlichen Auseinandersetzungen führen kann.

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

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

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

Kommentar:

Neben den rein wirtschaftlichen Gesichtspunkten der IT-Beschaffung sollten vor allem auch entsprechende Mindestanforderungen an die technische Qualität der beschafften Güter gestellt werden, um einen sicheren IT-Betrieb zu gewährleisten. Die Sicherstellung der Verfügbarkeit der Daten ist als ein zentraler Sicherheitsaspekt zu beachten.

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

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

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

Beim Einsatz netzwerkweit operierender Installations- und Inventarisierungswerkzeuge sind besondere Maßnahmen zum Schutz vor Missbrauch zu ergreifen. Insbesondere müssen verbindliche Regelungen getroffen werden, die sicherstellen, dass die Werkzeuge ausschließlich für diesen Zweck eingesetzt werden. Dazu muss u. a. festgelegt sein, dass die Werkzeuge nur auf dafür

bestimmten, besonders abgesicherten Arbeitsplätzen eingesetzt werden. Der Personenkreis, der berechtigt ist, diese Werkzeuge zu nutzen, ist auf das notwendige Maß zu beschränken. Die Anwender sind vor dem Einsatz solcher Werkzeuge zu informieren. Ihr Einsatz muss protokolliert und dokumentiert werden.

Kommentar:

Die Mehrzahl der an der Freien Universität Berlin betriebenen Rechner ist vernetzt. Auf dieser Basis ist die Zentralisierung von Diensten mit einer Reihe von ökonomischen Vorteilen verbunden. Zum einen werden die mit der Installation und dem Support beauftragten Stellen von aufwendigen Vorort-Arbeiten befreit, zum anderen werden die zuständigen Mitarbeiter beispielsweise von Sicherungsaufgaben entlastet. Grundsätzlich gilt, je stärker Zentralisierungs- und Automatisierungsprozesse tägliche Arbeitsabläufe bestimmen, desto höher ist das denkbare Missbrauchspotential. Um Akzeptanz für Zentralisierungen bei den Betroffenen zu schaffen bzw. zu erhöhen, sollte das Missbrauchspotential beispielsweise durch Dienstvereinbarungen ausgeschlossen werden.

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

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

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

Kommentar:

Ziel des an der Freien Universität Berlin etablierten Sicherheitsprozesses ist nicht nur das Erreichen des angestrebten Sicherheitsniveaus, sondern vor allem dessen dauerhafter Bestand und Verbesserung. Die Gewährleistung des Ziels kann durch die Umsetzung verschiedener Schritte erreicht werden. Insbesondere ist es sinnvoll, die IT-Sicherheitsmaßnahmen regelmäßig (z.B. alle zwei Jahre) auf ihre Effektivität und Umsetzbarkeit zu prüfen und ggf. den technischen und organisatorischen Gegebenheiten sowie neuen sicherheitstechnischen Anforderungen und Erkenntnissen anzupassen. Nur durch die konsequente und stetige Anpassung bzw. Korrektur kann das IT-Sicherheitsniveau wirksam aufrechterhalten werden.

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

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

Bei der Einführung neuer IT-Verfahren bzw. neuer IT-Arbeitsprozesse werden im Rahmen der Dokumentationspflichten Analysen zur Ermittlung des Schutzbedarfs und ggf. zur Identifizierung und Begegnung spezifischer Risiken vorgenommen. Basierend auf den Ergebnissen dieser Analysen sollte ein Notfallplan erstellt werden, in dem festgelegt wird, wie auf Notfallsituationen adäquat reagiert wird. „Notfall“ bezeichnet eine Situation, in der durch eine Betriebsstörung die Verfügbarkeit, Integrität oder Vertraulichkeit der Daten nicht mehr gegeben ist und ein verhältnismäßig hoher Schaden entsteht. In einem Notfallplan sollten zum Beispiel Regelungen zu Verantwortlichkeiten, zum Wiederanlauf von IT-Systemen, zur Wiederherstellung von Daten und zum Einsatz von Ausweichmöglichkeiten enthalten sein. Darüber hinaus ist es häufig sinnvoll einen Alarmierungsplan zu erstellen, in dem die Meldewege im Notfall beschrieben sind.

Kommentar:

Ziel dieser Maßnahme ist es sicherzustellen, dass mögliche Risiken z.B. durch den Ausfall des betrachteten Systems erkannt werden und über geeignete Maßnahmen nachgedacht wird, die im Notfall befolgt werden sollen. Je komplexer das System und je sensibler die verarbeiteten Daten, desto detaillierter sollte der Notfallplan gestaltet sein.

1.1.3. Personelle Maßnahmen

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

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

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	Bereichsleitung

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

Kommentar:

Befristet beschäftigte Mitarbeiter (Beschäftigungsverhältnis von deutlich weniger als einem Jahr) sollten nach Möglichkeit keine Aufgaben übernehmen, die nur mit Administratorrechten ausgeführt werden können. Besonders sicherheitskritische Aufgabengebiete, die zentrale Bedeutung für die Aufrechterhaltung des gesamten IT-Betriebs eines Bereiches haben, sollten von qualifizierten und verlässlichen, nach Möglichkeit fest angestellten Mitarbeitern wahrgenommen werden. Je sensibler das Aufgabenfeld, desto wichtiger ist die Beachtung dieser Maßnahme.

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

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

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

Kommentar:

Im Rahmen verschiedener Risikoanalysen hat sich immer wieder gezeigt, dass in bestimmten Fällen die Personalausstattung ungenügend ist. Dieser Personalmangel äußert sich u. a. häufig in der Vernachlässigung der Dokumentationspflichten sowie in unzulänglichen Vertretungsregelungen. Ein besonders kritischer Zeitpunkt ergibt sich in der Urlaubszeit bei gleichzeitig hohem Krankenstand. Die daraus resultierende hohe Arbeitsbelastung für die verbliebenen Mitarbeiter wirkt sich ungünstig auf einen reibungslosen IT-Betrieb bis hin zur Beeinträchtigung der Aufgabenerfüllung aus.

- **Vertretung (M2.15)**

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

Für alle Betreuungs- und Administrationsfunktionen sind Vertretungsregelungen erforderlich. Die Vertreter müssen alle notwendigen Tätigkeiten ausreichend beherrschen und ggf. auf schriftliche Arbeitsanweisungen und Dokumentationen zurückgreifen können. Die Vertretungsregelung muss im System abgebildet sein und darf nicht durch die Weitergabe von Passwörtern erfolgen.

Die technischen Voraussetzungen für die Wahrnehmung einer Vertretung sollten möglichst ständig eingerichtet sein. Eine Ausnahme bilden systemspezifische, nicht nutzerabhängige Kennungen (zum Beispiel *root* bei UNIX-

Systemen). Dort soll der Vertreter nur im Bedarfsfall auf das an geeigneter Stelle hinterlegte Passwort des Administrators zurückgreifen können.

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

Kommentar:

Die Intention dieser Maßnahme ist eng mit der Maßnahme „Angemessene Personalausstattung" verknüpft. In Situationen, in denen vorhersehbar (z.B. Urlaub) oder unvorhersehbar (z.B. Krankheit) Personalausfälle zu verzeichnen sind, muss durch angemessene Vertretungsregelungen die Fortführung der Arbeitsprozesse gewährleistet bleiben. Dazu sollte schon im Vorfeld festgelegt sein, wer wen in welchen Angelegenheiten vertritt. Diese Festlegungen sind besonders im IT-Bereich von grundlegender Bedeutung, da aufgrund des häufig benötigten Spezialwissens, die Einarbeitung in spezielle Aufgabengebiete sehr zeitaufwendig sein kann.

Um die Eindeutigkeit der Verantwortlichkeiten zu wahren, sollten Vertretungsregelungen organisatorisch und ggf. technisch verankert sein.

- **Qualifizierung (M2.16)**

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

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

Kommentar:

Ein störungsfreier IT-Einsatz kann nicht einzig und allein durch das Festlegen von Regelungen gewährleistet werden. Um für den Ernstfall gerüstet zu sein, ist es nicht nur wichtig Regelungen zu haben – diese sollten auch fachgemäß und effektiv umgesetzt werden. Vor allem sollte jedem Mitarbeiter bewusst sein, dass die Einhaltung und Umsetzung der Sicherheitsziele und -maßnahmen sowie der dauerhafte Bestand und die Steigerung des etablierten Sicherheitsniveaus ein Teil der täglichen Arbeitsroutine sind. Die Nutzung von Fortbildungsmöglichkeiten (auch ohne explizite Aufforderung durch einen Vorgesetzten) zählt ebenso dazu.

1.1.4. Sicherung der Infrastruktur

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

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

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

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

Kommentar:

In Abhängigkeit des Schutzbedarfs der Daten, die auf den Systemen verarbeitet werden, sollten Serverräume durch eine Vielzahl von unterschiedlichen Maßnahmen vor unbefugtem Zutritt, elementaren Schadensereignissen sowie Verlust der Verfügbarkeit gesichert werden. Zu nennen sind u.a. Sicherungsmaßnahmen in Form von baulichen Zutrittsbeschränkungen, Zutrittsregelungen und -kontrollmechanismen, die Auswahl geeigneter Gebäude und Räume, redundante Auslegung der infrastrukturellen und technischen Einrichtungen, das Vermeiden der Lagerung brennbarer Materialien im Serverraum sowie ein Nutzungsverbot von tragbaren IT-Systemen, Kameras und Mobiltelefonen, die nicht für die Belange der Freien Universität Berlin eingesetzt werden.

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

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

Der unbefugte Zugang zu Geräten und die Benutzung der IT muss verhindert werden. Bei Abwesenheit des IT-Personals sind Räume mit IT verschlossen zu halten. Es muss gewährleistet sein, dass Schlüssel nur an die jeweils berechtigten Personen ausgegeben werden. Bei der Anordnung und Einrichtung der Geräte ist darauf zu achten, dass Daten mit internen oder vertraulichen Inhalt nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

Kommentar:

Um auf Daten zuzugreifen, die auf einem Arbeitsplatz-PC abgelegt sind, ist normalerweise eine Anmeldung mit Benutzername und Passwort notwendig. Gegen den Diebstahl von Endgeräten sind jedoch weitere Vorkehrungen zu treffen. Insbesondere Geräte von zentraler Bedeutung, wie beispielsweise Server, auf denen jegliche Daten und Dateien aller Mitarbeiter eines Bereiches gespeichert sind, müssen besonders geschützt werden. Drucker sollten so platziert sein, dass vertrauliche Ausdrucke, z.B. Schreiben, die Personalangelegenheiten beinhalten oder wichtige Präsidiumspapiere, die nicht für die Öffentlichkeit bestimmt sind, nicht von jedermann eingesehen werden können.

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

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

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

Kommentar:

Um vertrauliche Dokumente oder z.B. spezielle Hardware zu schützen, bietet sich die Verwendung von Schutzschränken an. Doch auch der beste Schutzschrank bietet keine Sicherheit, wenn er nicht richtig aufgestellt und benutzt wird.

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

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

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

Kommentar:

Ähnlich wie in der Maßnahme 2.17 beschrieben, müssen spezielle Sicherheitsvorkehrungen, insbesondere für die Sicherung zentraler Netzknoten getroffen werden. Durch den an der Freien Universität Berlin vorherrschenden hohen Vernetzungsgrad von Arbeitsplatz-PCs als auch von Abteilungen sind Arbeitsplätze mit Stand-Alone-PCs kaum noch vorhanden. Folglich träfe ein möglicher Ausfall der Systeme nicht nur eine Minderheit der Mitarbeiter, sondern zum Beispiel ganze Abteilungen der Verwaltung, die in der Durchführung ihrer Arbeitsprozesse beeinträchtigt werden könnten.

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

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

Die Verkabelung des LAN ist klar zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Netzwerkadministratoren müssen einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung zentraler Komponenten haben. Nicht benutzte Anschlüsse sollten abgeklemmt oder deaktiviert werden. Erweiterungen und Veränderungen an der Gebäudeverkabelung, auch die Inbetriebnahme von Funknetzen, sind mit den IT-Verantwortlichen der eigenen Organisationseinheit und mit dem Hochschulrechenzentrum abzustimmen.

Kommentar:

Für die Gewährleistung eines ordnungsgemäßen Rechnerbetriebs ist anlässlich der Komplexität der an der Freien Universität Berlin betriebenen Netzstruktur eine umfassende und vollständige Dokumentation der Netze notwendig. Damit die IT-Verantwortlichen gerecht werden können, müssen sie frühzeitig über alle Planungen und Änderungen informiert und einbezogen werden. Die Bereiche, die ihre Netze eigenverantwortlich umstrukturieren bzw. erweitern wollen, müssen ihre Projekte mit der ZEDAT koordinieren.

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

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

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

Kommentar:

Gerade in Räumen mit Publikumsverkehr und in Bereichen, die unübersichtlich gestaltet sind, ist es zweckmäßig, Leitungen und Verteiler zu sichern. Denn zumeist sind weniger vorsätzliche Handlungen Ursache von Zerstörungen, als vielmehr die ungeschickte Kabelverlegung. Eine geschützte Kabelverlegung soll zum einen entsprechenden Schutz von Korrosion usw. bieten, zum anderen gezielte Angriffe, wie beispielsweise das Abhören von Telefongesprächen, verhindern. Wenn auch grundsätzlich eine vertrauliche Kommunikation zu verschlüsseln ist, muss bei der Verlegung der Leitungen darauf geachtet werden, dass diese nicht völlig ungeschützt und offen verlegt werden.

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

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

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

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

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

Kommentar:

Die Umsetzung der Maßnahme soll verhindern, dass Reinigungs- oder Fremdpersonal durch die unsachgemäße Behandlung der IT bzw. durch den Diebstahl von Geräten, materielle und finanzielle Schäden verursachen. Denn nicht selten kommt es vor, dass beispielsweise Reinigungspersonal wichtige Dokumente verlegt oder gar entsorgt oder durch „Spielen“ bzw. „Ausprobieren“ IT-Komponenten zerstört werden.

Externe Mitarbeiter, die längerfristig für die Freie Universität Berlin tätig sind, sollten in sämtliche, sie betreffende Aufgaben eingewiesen und insbesondere auch mit den geltenden Sicherheitsmaßnahmen vertraut gemacht werden. Auch für diese Mitarbeiter sollte es Vertretungsregelungen geben. Nach Beendigung des Arbeitsverhältnisses sind jegliche Zugriffsberechtigungen zu entziehen, Dokumente zu übergeben. Externe Mitarbeiter, die nur kurzfristig zum Einsatz kommen, sollten wie Besucher behandelt werden und in Folge dessen nicht unbeaufsichtigt in sicherheitskritische Bereiche vordringen dürfen.

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

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

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

Kommentar:

Trotz einer hohen Versorgungssicherheit können Stromunterbrechungen nicht gänzlich ausgeschlossen werden. Schon kurze Unterbrechungen von 10 Millisekunden reichen aus, um den IT-Betrieb zu stören. Auch Kabelbeschädigungen bei Tiefbauarbeiten oder unangekündigte Stromabschaltungen können zu einem Verlust der Verfügbarkeit von IT-Systemen führen. Die Aufwendungen, die für eine ausreichend abgesicherte Stromversorgung betrieben werden, sind von der notwendigen Verfügbarkeit der Dienste abhängig. Dienste, die für die Aufrechterhaltung der Geschäftsprozesse zentral sind, sollten daher mit einem Notstromaggregat abgesichert werden.

- **USV (M2.25)**

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

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

Kommentar:

Die Ursachen für Spannungsschwankungen können vielfältig sein. Beispielsweise können Störungen in den Netzen der Energieversorgungsunternehmen, aber auch Defekte an den an der Freien Universität Berlin installierten IT-Systemen zu solchen Schwankungen führen. Sinn der Maßnahme ist es, die durch Schwankungen in der Energieversorgung verursachten Funktionsstörungen bzw. Schäden an IT-Komponenten zu verhindern.

- **Brandschutz (M2.26)**

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

Die Regeln des vorbeugenden Brandschutzes sind zu beachten und einzuhalten. Insbesondere gilt dies für Räume mit wichtiger Informationstechnik, wie beispielsweise Serverräume. Papierlager, leere Verpackungen und andere leicht entflammbare Materialen dürfen in diesen Räumen nicht gelagert werden. In diesen Räumen sowie in anderen Technikräumen besteht Rauchverbot. Die Türen zu diesen Räumen sollen brandhemmend ausgelegt sein. In diesem Zusammenhang sind die Schutzklassen T30, T60, T90, T120 und T180 zu nennen. Außerdem sind Brandmelder und Handfeuerlöscher (Brandklasse B, CO_2-Löscher) vorzusehen. Für Hinweise und eingehende Beratung wenden Sie sich an Ihren örtlichen Brandschutzbeauftragten.

Kommentar:

Weitere Hinweise und Reglungen zum Thema Brandschutz finden sich auf der Homepage des Sicherheitsbeauftragten der Freien Universität Berlin. An dieser Stelle soll darauf hingewiesen werden, dass die Beachtung der Brandschutzmaßnahmen ebenso für kleine Räume, in denen konzentriert IT gelagert wird (z.B. in Bereichen, wo keine speziellen Serverräume zu diesem Zweck verwendet werden), gilt.

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

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

IT-Systeme, die wichtige oder unverzichtbare Komponenten zur Aufrechterhaltung eines geordneten Betriebes sind, sind nicht in direkter Nähe zu oder unter wasserführenden Leitungen aufzustellen. Auch bei einem Wassereinbruch muss der weitere Betrieb der IT-Systeme gewährleistet sein, dies gilt insbesondere dann, wenn die IT-Systeme in Kellerräumen aufgestellt werden. So ist beispielsweise besonders darauf zu achten, dass nicht die tiefste Stelle im Gebäude zur Aufstellung der Geräte genutzt wird.

Kommentar:

Die Folgen von Wasserschäden, wie beispielsweise Kurzschlüsse, Rost, Beschädigungen und Komplettausfälle, sind in geeigneter Weise abzuwehren.

- **Klimatisierung (M2.28)**

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

Der Einbau von Klimatisierungsanlagen wird erforderlich, wenn der Luft- und Wärmeaustausch von Server- und Rechnerräumen unzureichend ist bzw. hohe Anforderungen an die Be- und Entfeuchtung eines Raumes gestellt werden. Die Gewährleistung der zulässigen IT-Betriebstemperatur und demzufolge die Sicherstellung des IT-Betriebs steht in engem Zusammenhang mit dem reibungslosen Einsatz von Klimatisierungsgeräten. Daher müssen die Geräte mit einer hohen Verfügbarkeit ausgestattet sein.

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

Kommentar:

Neben der Stromversorgung spielt die Klimatisierung eine wichtige Rolle, da der größte Teil der zugeführten Energie in Form von Wärme wieder abgegeben wird. Gerade in den Sommermonaten kann es eine große Herausforderung sein, Temperatur und Luftfeuchtigkeit im Idealbereich zu halten. Die Miniaturisierung der Hardware und die steigende Leistungsfähigkeit der Geräte lassen herkömmliche Klimatisierungskonzepte oftmals an ihre Grenzen stoßen. Wie auch bei der Stromversorgung müssen bei der Klimatisierung Überkapazitäten geschaffen werden, damit bei einem (Teil-)Ausfall der Infrastruktur entstehende Versorgungslücken durch die Zuschaltung weiterer Anlagen kompensiert werden können.

1.1.5. Hard- und Softwareeinsatz

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

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

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

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

Kommentar:

Bei der Beschaffung spielen unterschiedliche Faktoren eine Rolle. Neben höherer Effizienz und Wirtschaftlichkeit können durch geregelte Beschaffungsverfahren auch Neu- und Weiterentwicklungen im Bereich der Informationstechnik stärker berücksichtigt sowie qualitative Anforderungen vereinheitlicht werden. Der Vorteil einer zentralen Beschaffungsstelle zeigt sich insbesondere bei der Frage nach der Kompatibilität einzelner IT-Komponenten. Durch Erfahrungswerte und gesicherte Informationsquellen ist eine zentrale Beschaffungsstelle viel eher in der Lage, Kompatibilitäts- und Qualitätsanforderungen zu beschreiben und IT dementsprechend zu einem guten Preis-Leistungsverhältnis zu beschaffen. Qualitativ hochwertige und kompatible IT-Systeme tragen ferner zu einer hohen Betriebssicherheit bei.

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

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

Auf Rechnersystemen der Freien Universität Berlin darf zum Zweck des Schutzes von universitätseigener Hardware und dem Universitätsnetz nur Software installiert werden, die von der zuständigen Stelle dafür freigegeben wurde. Bei der Freigabe muss darauf geachtet werden, dass die Software aus zuverlässiger Quelle stammt und dass ihr Einsatz notwendig ist. Das eigenmächtige Einspielen, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn eine Genehmigung der zuständigen Stelle vorliegt oder eine Organisationseinheit eine pauschale Freigabe für Teilbereiche festgelegt hat. Rechnersysteme sind gegen das unbefugte Herunterladen hard- und softwaretechnisch zu schützen.

Kommentar:

Die Anmeldung und Freigabe von Software sollte auf organisatorischer Ebene gewährleistet sein, mit dem Ziel, Sicherheitsrisiken, die sich durch nicht angemeldete IT-Komponenten ergeben können, auszuschließen.

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

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

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

Kommentar:

Grundsätzlich sind mit allen Entwicklungsarbeiten Gefahren für die IT-Sicherheit verbunden, da Seiteneffekte auftreten können, die im Vorfeld nicht abschätzbar sind. Aus diesem Grund wird eine strikte Trennung von Entwicklungs- und Produktivsystemen für sinnvoll erachtet.

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

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

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

Kommentar:

Software, die relativ komplex und umfangreich ist und deren Installation weitreichende und unvorhersehbare Konsequenzen nach sich ziehen kann, stellt eine erhebliche Gefährdung für den IT-Betrieb dar und muss folglich ein entsprechendes Test- und Freigabeverfahren durchlaufen. Der Aufwand für solche Tests ist häufig erheblich geringer, als der potentielle Aufwand für die Beseitigung möglicher Schäden und die Wiederherstellung der IT-Sicherheit.

Beispiel: Zuweilen kann es sinnvoll sein, Sicherheitsupdates nicht sofort zu installieren, sondern abzuwarten, bis Aussagen über die Updates im Internet verfügbar sind. Grund hierfür sind Probleme, die sich nach dem Einspielen solcher Sicherheitspatches ergeben können. Jedoch sollte stets abgewogen werden, welche Bedeutung und Dringlichkeit das Einspielen des Sicherheitsupdates zur Wiederherstellung der IT-Sicherheit hat.

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

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

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

Kommentar:

Die Formulierung dieser Maßnahme resultiert aus den Erfahrungen von Beschäftigten, die bereits an größeren Softwareentwicklungsprojekten teilgenommen bzw. derartige Projekte verwaltet und durchgeführt haben. Eine entsprechende Vorgehensweise ist gerade bei großen Projekten mit einer Vielzahl involvierter Mitarbeitern erforderlich, um die Übersicht über die verschiedenen Teilprojekte, deren Koordination und effektive Zusammenführung zu gewährleisten.

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

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

Auf allen Arbeitsplatz-PCs ist, soweit möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Jede Organisationseinheit ist verpflichtet, Virenschutzsysteme anzubieten. Durch den Einsatz von Virenschutzsystemen soll das Eindringen von schädlichem Programmcode erkannt und verhindert werden. Regelmäßig (möglichst automatisiert) sind die Virenerkennungsmuster zu aktualisieren. Wird auf ei-

nem System schädlicher Programmcode entdeckt, muss dies der zuständigen Stelle gemeldet und das Ergebnis der eingeleiteten Maßnahmen dokumentiert werden.

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

Kommentar:

Um einen höchstmöglichen Schutz vor Schadprogrammen zu erreichen, ist es sinnvoll, zu prüfen, inwieweit eine Kombination unterschiedlicher, aufeinander abgestimmter Anti-Virenschutzprogramme genutzt werden kann. Beispielsweise kann auf den Arbeitsplatz-PCs eines Bereiches ein Virenschutzprogramm des Herstellers A installiert werden, währenddessen auf den Fileservern ein Virenschutzprogramm des Herstellers B eingerichtet wird. Durch ein solches Verfahren steigt die Wahrscheinlichkeit alle bzw. möglichst viele Viren zu erkennen. Aus organisatorischer Sicht ist die Erarbeitung eines Virenschutzkonzeptes empfehlenswert, in dem alle Virenschutzmaßnahmen dokumentiert werden. Durch die übersichtliche Darstellung aller Maßnahmen können Schwachstellen aufgedeckt und durch entsprechende Schritte beseitigt werden.

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

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

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

Kommentar:

Mit Hilfe so genannter Einschubvorrichtungen bzw. durch den Ausbau von Laufwerken kann verhindert werden, dass PCs oder Server unkontrolliert gebootet und Daten unberechtigt auf externe Datenträger kopiert werden sowie Software unkontrolliert installiert wird. Bei aller Vorsicht sollte jedoch stets die Angemessenheit der Maßnahme beachtet werden, d.h. die Beschäftigten sollten nicht unnötig in der Ausführung ihrer Arbeit behindert werden.

- **Dokumentation (M2.36)**

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

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

Kommentar:

Eine fehlende oder unzureichende Dokumentation kann im Ernstfall erhebliche Konsequenzen für den Betrieb der IT-Komponenten nach sich ziehen. Beispielsweise kann eine Fehlerdiagnose bzw. -behebung bei Hardwareausfällen und Programmfehlfunktionen gar nicht oder nur unter erschwerten Bedingungen durchgeführt werden.

Beispiel: Die Installation neuer Software führt dazu, dass bestehende Konfigurationen geändert werden. In Folge dieser Änderung stürzen andere, bisher fehlerfrei laufenden Programme aufgrund falscher Parametrisierung ab. Eine detaillierte Dokumentation der vorgenommenen Installation einschließlich der Änderungen ist Grundlage für die schnelle Lokalisierung und Behebung des Fehlers.

- **Ausfallsicherheit (M2.37)**

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

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

Kommentar:

Die Maßnahmen für das Erreichen einer entsprechenden Ausfallsicherheit von IT-Systemen richten sich nach der Verfügbarkeit der Daten. Das bedeutet, dass sowohl Systeme oder Komponenten von IT, als auch Netze, deren Ausfall in einer Weise die Verfügbarkeit beeinträchtigen können, beispielsweise durch Wartungsverträge, redundante Auslegung von Netzen usw. gesichert werden müssen.

Beispiel: Zum Ende des Anmeldezeitraums für die Buchung von Lehrveranstaltungen ist neben der Verfügbarkeit des Campus Management Systems besonders wichtig, dass nicht nur die betroffenen Server problemlos laufen, sonders ebenso die Netze verfügbar sind.

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

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

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

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

Kommentar:

Da mobile PCs besonders stark von Diebstahl bedroht sind, ist es sehr wichtig, dass Daten z.B. durch Verschlüsselung gegen unbefugte Einsicht geschützt werden. Damit bleiben auch bei Verlust des Gerätes die Daten für Außenstehende unzugänglich. Außerdem ist eine geeignete Regel zur Übergabe zu vereinbaren, um ständig nachvollziehen zu können, wer das Gerät wo benutzt.

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

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

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

Kommentar:

Der Diebstahl von IT-Komponenten führt neben dem Verlust der Verfügbarkeit zu teilweise immensen Wiederbeschaffungskosten und verursacht personelle Aufwendungen, die zur Wiederherstellung eines arbeitsfähigen Zustandes notwendig werden. Neben diesen ökonomischen Konsequenzen müssen vor allem der Verlust der Vertraulichkeit der Daten und die daraus resultierenden Folgen bedacht werden.

1.1.6. Zugriffsschutz

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

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

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

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

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

Kommentar:
Um zu verhindern, dass aus einem IT-System schutzbedürftige Daten ausgelesen werden können, sollte ein Verschlüsselungsprogramm eingesetzt werden. Mit Hilfe der marktgängigen Produkte ist es möglich, einzelne Dateien, bestimmte Bereiche oder die ganze Festplatte so zu verschlüsseln, dass nur derjenige, der über den geheimen Schlüssel verfügt, in der Lage ist, die Daten zu lesen und zu gebrauchen.

Die Sicherheit der Verschlüsselung hängt dabei von drei Punkten zentral ab:

- *Der verwendete Verschlüsselungsalgorithmus muss so konstruiert sein, dass es nicht möglich ist, diesen zu brechen, d.h. dass der nötige Aufwand in keinem Verhältnis zum erzielten Informationsgewinn steht.*
- *Der Schlüssel ist geeignet zu wählen. Wenn möglich sollte er zufällig erzeugt werden.*
- *Der Verschlüsselungsalgorithmus, die verschlüsselten Daten und der Schlüssel dürfen nicht zusammen auf einem Datenträger gespeichert wer-*

den. Es bietet sich an, den Schlüssel einzeln aufzubewahren (z.B. auf einer Chipkarte oder einem USB-Stick gespeichert in der Brieftasche).

Achtung: ein verlorener bzw. vergessener Schlüssel bedeutet den vollständigen Datenverlust und kommt einem unwiederbringlichen Löschen der Daten gleich!

- **Netzzugänge (M2.41)**

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

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

Kommentar:

Prinzipiell ist das unberechtigte Anschließen von IT-Systemen an Datennetze der Freien Universität Berlin kaum zu verhindern und bleibt meistens auch unbemerkt. Die Auswirkungen einer unberechtigten Rechnerintegration können sämtliche Netzsegmente betreffen und einen immensen Schaden nach sich ziehen. Aufgrund des hohen Missbrauchspotentials ist die Umsetzung der Maßnahme von besonderer Bedeutung.

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

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

Alle IT-Systeme und Anwendungen sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist eine Anmeldung mit Benutzerkennung und Passwort erforderlich. Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel personenbezogen erfolgen. Die Arbeit unter der Kennung einer anderen Person ist unzulässig. Dem Benutzer ist untersagt, Kennungen und Passwörter weiterzugeben.

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

Kommentar:

In standardmäßig abgesicherten Systemen sind die Benutzer-Passwort-Kombinationen die einzige Hürde für den Zugriff auf die verarbeiteten Daten. Insbesondere aus diesem Grund sollten die Benutzer in Hinblick auf einen angemessenen Umgang mit personenbezogenen Kennungen entsprechend sensibilisiert werden. Daneben können durch die Organisation des Identitätsmanagements beispielsweise Redundanzen vermieden werden.

- **Administratorkennungen (M2.43)**

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

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

Kommentar:

Ausgehend von den weitreichenden Handlungsmöglichkeiten, die der Besitz einer Administratorkennung eröffnet und dem damit verbundenen Missbrauchspotential, ist anzunehmen, dass besonders solche Kennungen das Ziel von Spionageangriffen sind. Aus diesem Grund sollten Administratorkennungen nur dann verwendet werden, wenn die Rechte zur Durchführung der Arbeitsaufgaben erforderlich sind. Ein kontinuierliches Arbeiten unter der Administratorkennung kann folgenschwere Auswirkungen nach sich ziehen, wie beispielsweise das unbeabsichtigte Löschen von Dokumenten.

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

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

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

System zwischen mehreren Personen geteilt, so ist nach dem Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.

Kommentar:

In der Vergangenheit war es die Regel, dass das zuständige IT-Personal nicht oder nur sporadisch über das Ausscheiden eines Mitarbeiters informiert wurde. Diese Maßnahme soll deshalb die erforderlichen Schritte festlegen und deren Einhaltung sicherstellen, um das von einem ausgeschiedenen Mitarbeiter ausgehende potentielle Sicherheitsrisiko zu minimieren.

- **Passwörter (M2.45)**

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

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

- Das Passwort darf nicht leicht zu erraten sein wie Namen, Kfz-Kennzeichen, Geburtsdatum.
- Das Passwort muss mindestens einen Buchstaben und mindestens eine Ziffer oder ein Sonderzeichen enthalten.
- Das Passwort sollte mindestens 8 Zeichen lang sein. Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
- Das Passwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.
- Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln.

- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.
- Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes muss unbeobachtet stattfinden.

Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern ("BBBBBB", "123456") sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpasswörtern.
- Nach dreifacher mehrfacher fehlerhafter Passworteingabe muss eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann. oder nach Ablauf einer Sperrfrist automatisch auf-gehoben wird.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Die Passwörter sollten im System zugriffssicher gespeichert werden, z. B. mittels Einwegverschlüsselung.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).

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

Kommentar:

Die besten technischen Authentifizierungsverfahren verlieren ihre Schutzwirkung, wenn die Anwender nicht sorgfältig mit den Passwörtern umgehen. Sicherheitslücken finden sich hauptsächlich in den folgenden drei Punkten:

- *Das Problem der Weitergabe: Passwörter werden weitergegeben oder unter Kollegen geteilt.*

- *Das Problem der unsicheren Aufbewahrung: Nicht selten werden Passwörter auf Zetteln vermerkt, die dann unter der Tastatur verstaut bzw. an den Bildschirm geklebt werden.*
- *Das Problem der Wahl des Passworts: Häufig werden besonders leicht zu merkende Passwörter gewählt, mit der Folge, dass diese den beschriebenen Kriterien entgegenstehen.*

Diesem Gefahrenpotential kann zum einen durch technische Maßnahmen, wie beispielsweise technische Kontrollen über die Einhaltung der Regelungen, begegnet werden, zum anderen ist es empfehlenswert, die Anwender über die Folgen des unzureichenden Passwortgebrauchs aufzuklären.

***Schwierige Passwörter leicht gemerkt**:*
Als IT-Personal sollten Sie Anwendern vermitteln, dass sich auch Passwörter, die nur sehr schwer zu knacken sind, leicht zu merken sind. Ein so genannter Algorithmus kann dabei helfen, immer ein anderes Passwort zu haben, das sich aber leicht herleiten lässt.

Beispiel: Sie haben zwei feste Bestandteile eines Passworts. In diesem Falle ZEDAT 07. Wenn Sie beispielsweise einen Account bei Amozon anlegen, könnten sie zwischen ZEDAT und 07 noch ein zon einfügen. (ZEDATzon07). Das Passwort könnte noch komplizierter gemacht werden, wenn Sie die Buchstabenanzahl von Amazon auch noch einfügen würden.

Genauere Informationen finden Sie unter: http://www.fu-berlin.de/zuv/eas/it-sicherheit/Tipps/index.html

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

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

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

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

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

zu wichtigen Systemen für die Anwender auf die üblichen Arbeitszeiten eingeschränkt werden.

Kommentar:

Soweit technisch möglich, sollten die Zugriffsrechte in einem IT-System so gewählt werden, dass die Benutzer alle Funktionen zur Erledigung ihrer Aufgaben zur Verfügung haben. Besitzt in einem komplexen System jeder Benutzer weitreichende Rechte, besteht die Gefahr, dass aus Versehen oder aus Neugierde Funktionen ausgelöst werden, deren Auswirkungen von den Benutzern nicht abgeschätzt werden können.

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

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

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass das zuständige IT-Personal über die notwendige Änderung der Berechtigungen eines Anwenders, z. B. in Folge von Änderungen seiner Aufgaben, rechtzeitig informiert wird, um die Berechtigungsänderungen im System abzubilden.

Kommentar:

Die Erläuterungen zu der Maßnahme M 2.42 gelten ebenso an dieser Stelle. Erfolgt keine Anpassung der Zugriffsrechte, ist der Benutzer in der Lage, Zugriffsrechte anzuhäufen, die ggf. nicht zur Durchführung der Arbeit benötigt werden.

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

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

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

Kommentar:

Nur wenn sich alle Nutzer nach Aufgabenerfüllung am IT-System abmelden, kann der Schutz mittels einer Zugriffskontrolle wirksam werden. Gelingt es unbefugten Personen unter der Identität eines anderen Zugriff zu IT-Systemen und Daten zu erlangen,

versagt jegliche Zugriffskontrolle. Es sollten auch dann Regelungen für die Abmeldung an IT-Systemen getroffen werden, wenn keine Zugriffskontrolle stattfindet, um sicherzustellen, dass Anwendungen und Dateien nach Aufgabenerfüllung geschlossen werden.

1.1.7. System- und Netzwerkmanagement

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

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

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

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

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

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

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

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

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

Kommentar:

Die Art und der Umfang einer Protokollierung hängen in der Regel vom Schutzbedarf der auf den IT-Systemen verarbeiteten Daten ab. Es gilt jedoch der Grundsatz der Datenvermeidung. Die Protokollierung von Zugangsdaten muss unter Beachtung der Datenschutzgesetze erfolgen, da es sich bei diesen Daten in der Regel um personenbezogene Daten handelt. Daher sollte auch die Einsichtnahme in Protokolle nach Möglichkeit auf einen kleinen Kreis beschränkt bleiben, wobei sichergestellt werden muss, dass die zugriffsberechtigten Personen die Bestimmungen des Datenschutzes kennen und beachten.

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

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

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

Kommentar:

Die Angemessenheit der Protokollierung muss gegeben sein. Unter Beachtung der Mitbestimmungsrechte sowie der Datenschutzgesetze kann die Protokollierung bestimmter Sachverhalte ein wirksames Mittel zur Erhöhung der Sicherheit darstellen.

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

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

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

Kommentar:

In Abhängigkeit der Brisanz der Daten bzw. bei Systemen, bei denen es ganz besonders darauf ankommt, festzuhalten, wer, wann, was gemacht hat, kann die Protokollierung der administrativen Tätigkeiten sinnvoll sein.

Beispiel: Die verschiedenen SAP-Anwendungen stellen häufig hohe Anforderungen an die Verfügbarkeit der Dienste sowie die Vertraulichkeit und Integrität der Daten. Aus Gründen der Nachvollziehbarkeit usw. werden die an diesen Systemen durchgeführten Tätigkeiten protokolliert.

1.1.8. Kommunikationssicherheit

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

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

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

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

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

Kommentar:

Diese Maßnahme trägt der Tatsache Rechnung, dass funktionierende Netze für fast alle Arbeitsprozesse von zentraler Bedeutung sind. Entsprechend dieser Bedeutung muss zum einen darauf geachtet werden, dass kompetente Mitarbeiter die Netzwerkadministration vornehmen, zum anderen die Netzwerkdokumentation unter Verschluss gehalten werden sollte.

- **Netzmonitoring (M2.53)**

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

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

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

Kommentar:

Ein umfassendes Netzmonitoring erleichtert das Erkennen von Netzspionage und Netzangriffen und ist somit für den reibungslosen IT-Betrieb unabdingbar.

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

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

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

Kommentar:

Um zu gewährleisten, dass nur berechtigte IT-Systeme und Rechner an das Netz der Freien Universität Berlin angeschlossen sind, ist es von großer Wichtigkeit, dass keine Ports offen gehalten werden, die von Unbefugten genutzt werden könnten. Diese Maßnahme allein kann zwar nicht garantieren, dass keine fremde Hardware an das Universitäts-Netz angeschlossen wird, sie trägt aber wesentlich dazu bei.

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

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

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

Kommentar:

Der Sinn der Maßnahme wird deutlich, wenn ein zu schützender IT-Bereich mit einem zu schützenden Haus verglichen wird. Die starke Absicherung des Vordereingangs durch eine massive Tür, die durch einen Pförtner überwacht wird ist sinnlos, wenn der Hintereingang weder verschlossen, noch überwacht wird. In diesem Beispiel wäre das Haus ein zu schützendes Teilnetz, der Vordereingang mit Pförtner wäre ein Firewall-System und der Hintereingang könnte z.B. ein innerhalb des Teilnetzes betriebenes Modem sein.

1.1.9. Datensicherung

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

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

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

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

Kommentar:

Der Schutzbedarf der Daten, insbesondere die Verfügbarkeitsanforderungen, das Datenvolumen sowie die Änderungsfrequenz der Daten sind nur einige Faktoren, die auf die Verfahrensweise zur Datensicherung Einfluss nehmen können und somit im Datensicherungskonzept berücksichtigt werden müssen. Gleichzeitig müssen die Aufwendungen wirtschaftlich vertretbar bleiben.

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

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

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

Kommentar:

Die Information der Anwender über Aspekte der Datensicherung ist besonders wichtig, da nur sie den Schutzbedarf der Daten kennen und demzufolge die Anforderungen an die Datensicherung definieren können. In Zusammenarbeit mit den Anwendern können dann auch für spezielle Anforderungen gesonderte Lösungen erarbeitet werden.

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

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

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

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

Kommentar:

Um Datenverluste zu vermeiden, müssen regelmäßige Datensicherungen durchgeführt werden. Ein sinnvolles Vorgehen besteht häufig darin, dass die Daten nicht auf den Arbeitsplatz-PCs gesichert werden, sondern auf zentralen Fileservern. Die Mitarbeiter sollten dementsprechend informiert werden, damit sie den Fileserver als zentrale Ablage für ihre Daten nutzen. In einem Datensicherungskonzept sollten die Reglungen dokumentiert sein, welche Daten von wem wann gesichert werden müssen.

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

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

Die Sicherung der Daten auf Servern sollte im angemessen Rhythmus erfolgen. Auch System- und Programmdaten sind nach Veränderungen zu sichern. Zur Datensicherung sind dafür geeignete Backup-Werkzeuge zu verwenden, die eine Datensicherung für Daten, deren Wiederherstellung mehr als einige Tage erfordert, nach dem Generationenprinzip unterstützen.

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

Kommentar:

Server, insbesondere Applikationsserver, sind für die Verfügbarkeit von Diensten von zentraler Bedeutung. Von einem Ausfall dieser Server sind häufig viele Mitarbeiter betroffen. Aufgrund dieser Bedeutung ist eine umfassende Datensicherung, in der nicht nur die Daten, sondern auch die Applikationen gesichert werden, besonders wichtig.

Die Art der Sicherung (Umfang, Zeitintervall, Generationenanzahl usw.) richtet sich einerseits nach dem Schutzbedarf der Daten, die auf dem Server verarbeitet bzw. gespeichert werden, anderseits nach der Häufigkeit der Modifikationen auf dem Server.

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

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

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

Kommentar:

In der Praxis ist es bereits vorgekommen, dass wichtige Daten zwar regelmäßig gesichert wurden, die Datensicherung aber nie überprüft wurde. Bei dem Versuch, die gesicherten Daten zurückzuspielen, wurde dann festgestellt, dass die Datensicherungen fehlerhaft sind. Für die Rekonstruktion eines Datenbestandes muss deshalb stichprobenartig geprüft werden, ob die angefertigten Datensicherungen benutzt werden können.

1.1.10. Datenträgerkontrolle

- **Aufbewahrung (M2.61)**

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

Die Sicherungsdatenträger sind getrennt vom jeweiligen Rechner aufzubewahren. Bei Datenbeständen ab Schutzklasse „hoch“ sind die Datenträger in einem anderen Gebäude, einer anderen Brandschutzzone oder in einem für Datenträger geeigneten feuersicheren Tresor aufzubewahren (Schutzklasse mind. S 60 Dis, derartige Tresore sind entsprechend gekennzeichnet).

Bei der Lagerung der Datenträger sind die Angaben der Hersteller, insbesondere zu Temperatur und Luftfeuchtigkeit zu beachten. Bei längerer Lagerung sind Vorkehrungen zu treffen, die eine alterungsbedingte Zerstörung der Datenträger verhindern. In angemessenen Zeitabständen ist ein Umkopieren der Daten auf neuere Datensicherungsträger vorzusehen. Die Fortentwicklung der Sicherungssysteme ist zu beachten. Bei einer Langzeitarchivierung muss ggf. die Bereitstellung eines Lesegeräts eingeplant werden, dass für die verwendeten Datenformate geeignet ist.

Kommentar:

Zusätzlich zu den genannten Maßnahmen sind noch weitere Aspekte zu berücksichtigen. So unterliegen beispielsweise Backup-Datenträger besonderen Anforderungen hinsichtlich ihrer Aufbewahrung.

- *Der Zugriff auf diese Datenträger darf nur befugten Personen möglich sein, so dass eine Entwendung ausgeschlossen werden kann.*
- *Ein ausreichend schneller Zugriff muss im Bedarfsfall gewährleistet sein.*

Eine besondere Problematik zeigt sich bei Langzeitarchivierungen. Da jedes Speichermedium eine endliche Speicherdauer besitzt, ist rechtzeitig, d.h. bevor das Auslesen der Daten nicht mehr erfolgen kann, die Übertragung auf neue Datenträger zu initiieren. Gleichzeitig muss das Vorhalten entsprechender Technik zum Wiederherstellen, Auslesen und Übertragen der Daten sichergestellt werden.

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

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

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

Kommentar:

Diese Maßnahme zielt besonders auf die Speicherung von schützenswerten oder hoch schützenswerten Daten auf mobilen Datenträgern ab. Grundsätzlich soll mit der Umsetzung der Maßnahme sichergestellt werden, dass auch nach mehreren Monaten oder Jahren stets erkennbar ist, dass auf bestimmten Datenträgern hochsensible Daten gespeichert sind. Damit lässt sich beispielsweise verhindern, dass CDs mit vertraulichen Daten einfach weggeschmissen werden.

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

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

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

Kommentar:

Wie bei der vorherigen Maßnahme zielt auch diese Maßnahme darauf ab, dass besonders schützenswerte Daten nicht in falsche Hände geraten.

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

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

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

Kommentar:

In Abhängigkeit vom Schutzbedarf der Daten muss eine angemessene Transportmethode gewählt werden. Bei der Übermittlung hochschützenswerter Daten sollte überlegt werden, ob die Möglichkeit besteht, die Daten verschlüsselt über Datennetze zu transportieren.

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

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

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

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

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

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

Kommentar:

Bei unsachgemäßem Löschen besteht die Gefahr, dass Daten ausgelesen bzw. rekonstruiert werden können. Um das Bekannt werden dieser Daten auszuschließen, müssen Datenträger adäquat, wie in den Maßnahmen für IT-Personal 1.19 geschildert, gelöscht werden. Die in letzter Zeit vermehrt auftretenden Presseberichterstattungen über den Umlauf von Datenträgern mit brisanten z.T. personenbezogenen Daten hat gezeigt, dass die Maßnahme mit Sorgfalt umzusetzen ist. Ein Bekannt werden von schützenswerten Daten aufgrund nicht durchgeführter Datenträgerlöschung gilt es zu verhindern, da es zum einen gegen Gesetze und Richtlinien verstößt, zum anderen beträchtliche Schäden verursachen kann.

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

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

Papiere mit vertraulichem Inhalt sind mit Hilfe eines Aktenvernichters zu vernichten. Bei der Beschaffung eines Aktenvernichters ist die DIN 32757 zu beachten. Alternativ kann die Entsorgung auch über einen Dienstleister erfolgen. In diesem Fall muss sichergestellt sein, dass der Auftragnehmer über entsprechende Zertifikate verfügt. Der Auftragnehmer ist zur Protokollierung der Aktenvernichtung zu verpflichten.

Kommentar:

Dass Papierausdrucke ebenso zur IT-Landschaft zählen, wird insbesondere im IT-Umfeld häufig vergessen. Jedoch sind Papierausdrucke mit schützenswertem Inhalt entsprechend dem Schutzbedarf der elektronischen Daten zu behandeln. Es sind folglich dieselben Regelungen anzuwenden, wie bei elektronischen Daten.