IT-Grundschutz

für die Bauhaus-Universität Weimar und die Hochschule für Musik FRANZ LISZT Weimar

Version 1.1

vom 06.06.2008

Inhalt

Definition des Grundschutzes

Die Prozesse in Forschung und Lehre, sowie der Verwaltung sind immer stärker vom ordnungsgemäßen Funktionieren der Informations- und Kommunikationstechnik abhängig. Gleichzeitig steigt die Zahl potentieller Bedrohungen sprunghaft an. Gefährdet sind insbesondere die Verfügbarkeit, die Integrität und die Vertraulichkeit von Informationen. Diese Begriffe werden auch als Grundwerte der IT-Sicherheit verstanden.

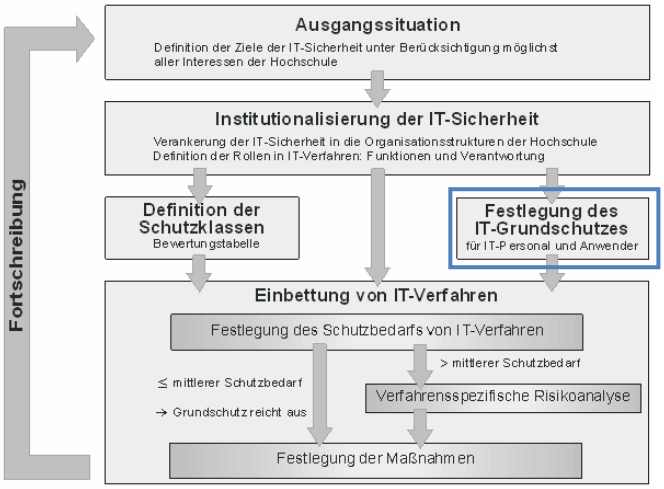

Abbildung 1: IT-Grundschutz im IT-Sicherheitsprozess

Um ein angemessenes IT-Sicherheitsniveau zu erreichen und aufrecht zu erhalten ist der IT-Sicherheitsprozess (siehe Abbildung 1) als übergreifende Arbeitsorganisation aus den Bereichen Infrastruktur, Personal, Hard- und Software, Kommunikation und Notfallvorsorge erforderlich. Das Sicherheits-Management-Team (SMT) beschließt auf Grundlage der bestehenden IT-Sicherheitsordnung den für beide Hochschulen verbindlichen und in diesem Dokument niedergelegten Maßnahmenkatalog.

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

Die Anwendung der hier für den Grundschutz zusammengestellten Standard-Sicherheitsmaßnahmen zielt darauf ab, ein Sicherheitsniveau für IT-Systeme zu erreichen, das für den normalen Schutzbedarf[1] angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann. Die Maßnahmen bilden die Grundlage für alle IT-Verfahren der Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT. Ihre Realisierung in den Bereichen wird mittelfristig Voraussetzung für die Teilnahme an zentralen IT-Verfahren wie z.B. E-Mail, Storage, oder Datensicherung sein.

Die Einhaltung der Vorgaben ist eine unverzichtbare Grundlage für den stabilen Einsatz der Informationstechnik, denn bereits ein ungeschütztes System kann eine Gefährdung für das gesamte Hochschulnetz darstellen. Mit einer auf eine lokale Betrachtung reduzierten Sichtweise erscheinen die beschriebenen Maßnahmen dem Einzelnen möglicherweise unbequem und übertrieben. Zahlreiche sicherheitsrelevante Vorfälle in der jüngeren Vergangenheit unterstreichen jedoch stark ihre Notwendigkeit. Beispielsweise kann die Verbreitung und das Wirksamwerden von

[1] frühere Bezeichnung: niedriger bis mittlerer Schutzbedarf

Schadsoftware, wie Viren, Würmern und Trojanischen Pferden über bereits bekannte Sicherheitslücken eingesetzter Standardsoftware durch den Einsatz aktueller Schutzprogramme und dem zeitnahen Einspielen der verfügbaren Programmaktualisierungen verhindert werden.

Ein durchdachtes Server- und Datensicherungskonzept kann wirksam vor den Folgen von Diebstählen von IT-Systemen aus schlecht gesicherten Gebäuden und dem damit einhergehenden unwiederbringlichen Verlust von wichtigen Daten schützen. Eine gute und klar strukturierte Organisation kann dazu führen, dass wichtige Informationen z.B. über Sicherheitslücken oder den Missbrauch von Rechnern zeitnah alle potentiell Betroffenen bzw. die IT-Verantwortlichen erreicht. So können Schäden und daraus resultierende Kosten vermieden werden.

Für IT-Verfahren mit hohem und sehr hohem Schutzbedarf müssen über die hier fixierten Grundschutzmaßnahmen hinaus zusätzliche, aus spezifischen Risikoanalysen abgeleitete und verfahrensbezogene Maßnahmen erarbeitet werden.

Die Maßnahmen des Grundschutzes werden gesondert für IT-Anwender und IT-Personal (wie IT-Betreuer und Systemadministratoren) dargestellt, wobei die Maßnahmen für IT-Personal als Ergänzungen zu den allgemeingültigen Maßnahmen für IT-Anwender zu verstehen sind. Der Maßnahmenkatalog wird zukünftig allen Anwendern an der Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT zugänglich und bekannt gegeben werden. Entsprechende Übergangsbestimmungen und Zeiträume zur Umsetzung sind vorzusehen.

Als Basis für die hier dargestellten IT-Grundschutzmaßnahmen dienten die IT-Grundschutz-Kataloge[2] des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die IT-Sicherheitsrahmenrichtlinie für die Freie Universität Berlin[3] und die Ergebnisse der Sicherheitsanalyse der Firma Litcos GmbH & Co. KG[4]. Bei der Erarbeitung der Grundschutzmaßnahmen für die Bauhaus-Universität Weimar und die Hochschule für Musik FRANZ LISZT wurden Anpassungen an die vorhandenen spezifischen Gegebenheiten vorgenommen. Für Detailinformationen zu einzelnen Maßnahmen wird die Lektüre der detaillierten Ausführungen der IT-Grundschutz-Kataloge empfohlen.

Zu jeder Regel und zu jeder Maßnahme sind Verantwortliche für die Initiierung und Verantwortliche für die Umsetzung konkret benannt.

„Verantwortlich für die Initiierung“ bezeichnet die Personen (als Rolleninhaber), die die Implementierung einer Maßnahme veranlassen sollen. „Verantwortlich für die Umsetzung“ bezeichnet die Personen (als Rolleninhaber), die die Maßnahme in der täglichen Praxis realisieren sollen. Bei der Initiierung muss unterschieden werden zwischen dem bereichsweise zuständigen IT-Verantwortlichen und dem Verfahrensverantwortlichen.

[2] Stand: Dezember 2005
[3] Fassung vom August 2005 (Version 1.9)
[4] Sicherheitschecks für den Bereich Bauausführung und den infrastrukturellen Anwendungen in den Network Centern 1-4 und dem Backup-Raum, durchgeführt am 03.08.2006

1. Begriffsdefinitionen

IT (= Informationstechnik)

Gesamtheit der technischen Mittel zur Erhebung, Erfassung, Aufbereitung, Nutzung, Speicherung, Übermittlung, programmgesteuerten Verarbeitung, internen Darstellung, Ausgabe und Wiedergewinnung von Daten.

IT-Verfahren

Gesamtheit von IT-gestützten Arbeitsabläufen und –prozessen, die eine arbeitsorganisatorisch abgeschlossene Einheit bilden.

IT-Sicherheitsprozess

Geplantes und organisiertes Vorgehen zur Durchsetzung und Aufrechterhaltung des angestrebten IT-Sicherheitsniveaus.

IT-Anwender (Benutzer, Nutzer, User)

Natürliche Person, die als Angehöriger oder Gast der Weimarer Hochschulen berechtigt IT verwendet.

IT-Personal (IT-Betreuer, Systemadministratoren)

Natürliche Person, die administrativen Aufgaben im laufenden IT-Betrieb wahrnimmt. Sie ist zuständig für Einrichtung, Betrieb, Überwachung und Wartung eines IT-Systems bzw. sie nimmt Benutzeranfragen zu Problemen rund um die IT-Ausstattung entgegen und bearbeitet sie.

IT-Verantwortlicher

Natürliche Person, die in Abstimmung mit der Bereichsleitung über die IT-Richtlinienkompetenz in ihrem Bereich verfügt und den IT-Einsatz einer Organisationseinheit der Bauhaus-Universität bzw. der Hochschule für Musik FRANZ LISZT koordiniert und plant, sowie die hochschulweit geltenden IT-Sicherheitsmaßnahmen umsetzt.

Bereichsleitung (Dekane, Abteilungsleiter, Leiter)

Leitung einer Organisationseinheit der Bauhaus-Universität Weimar bzw. der Hochschule für Musik Franz Liszt die die Verantwortung für den IT-Einsatz in ihrem Aufgabenbereich trägt. Sie benennt IT-Verantwortliche, die in ihrem Auftrag und mit ihrem Einverständnis den IT-Einsatz koordiniert und plant und darüber hinaus die hochschulweit geltenden IT-Sicherheitsnahmen umsetzt. Die Bereichsleitung ist zuständig für alle bereichsinternen IT-Planungen und für den laufenden internen IT-Betrieb. In diesem Rahmen ist die Bereichsleitung auch verantwortlich für die Umsetzung hochschulweiter IT-Richtlinien.

Verfahrensverantwortlicher

Der IT-Verfahrensverantwortliche trägt die Gesamtverantwortung für ein oder mehrere spezielle IT-Verfahren und ist für den korrekten Ablauf verantwortlich. Er ist der Besitzer der im Verfahren verarbeiteten Daten und bestimmt den Schutzbedarf seines/ seiner Verfahren.

2. Maßnahmen des IT-Grundschutzes für IT-Anwender

2. 1 Allgemeines

Anwenderqualifizierung (M 1.1)

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

Vor der Übernahme IT-gestützter Aufgaben sind die Benutzer zeitnah und ausreichend zu schulen. Dabei müssen sie in die Benutzung der für den Arbeitsplatz wesentlichen IT-Systeme und IT-Anwendungen eingewiesen werden. Außerdem sind sie mit den für sie relevanten Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes vertraut zu machen. Bei umfangreichen Änderungen in einer IT-Anwendung müssen darüber hinaus Schulungsmaßnahmen durchgeführt werden. An Stelle einer Schulung kann hier auch die Forderung nach selbständiger Einarbeitung stehen, wenn leicht verständliche Handbücher (ggf. in elektronischer Form) zur Verfügung gestellt werden und eine ausreichende Einarbeitungszeit gewährt wird.

Einhaltung einschlägiger Regelungen und Ordnungen (M 1.2)

Verantwortlich für Initiierung:	Hochschulleitungen, IT-Sicherheits-Management-Team
Verantwortlich für Umsetzung:	IT-Verantwortlicher (bereichsspezifisch), IT-Verfahrensverantwortlicher (verfahrensspezifisch)

Die Benutzer sollten die einschlägigen internen Regelungen und Ordnungen für die Benutzung der Informationstechnik[5] kennen, insbesondere die Ordnung für die Nutzung der IV-Infrastruktur der Bauhaus-Universität Weimar und haben diese einzuhalten.

Meldung von Sicherheitsvorfällen (M 1.3)

Verantwortlich für Initiierung:	Hochschulleitungen (Fachbeirat SCC)
Verantwortlich für Umsetzung:	IT-Verantwortlicher/ dezentraler IT-Sicherheitsbeauftragter (bereichsspezifisch), IT-Verfahrensverantwortlicher (verfahrensspezifisch)

Auftretende Sicherheitsvorfälle aller Art (Systemabstürze, Fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle und -beschädigungen, Eindringen Unbefugter, Manipulationen, Virenbefall etc.) sind dem zuständigen IT-Personal unverzüglich zu melden und, falls erforderlich, zur Vermeidung von Folgestörungen, Unfällen und Bränden das System kenntlich zu sperren. Gegenmaßnahmen dürfen erst nach Aufforderung durch Berechtigte ergriffen werden. Jeder schwerwiegende Vorfall ist zu dokumentieren. Informationen über Sicherheitsvorfälle dürfen nicht unautorisiert an Dritte weitergegeben werden.

[5] Veröffentlicht unter: http://www.uni-weimar.de/cms/?id=regelungen

2. 2 Sicherung der Infrastruktur

Räumlicher Zugangsschutz (M 1.4)

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender, Servicezentrum Liegenschaften, als Vertragspartner mit externen Dienstleistern (Reinigungskräften, Servicetechnikern etc.)

Der unbefugte Zugang zu IT-Systemen und die unautorisierte Benutzung von Informationstechnik muss verhindert werden. Der Zugang ist über Zutrittsregelungen zu sichern, zum Beispiel über eine Schlüsselverwaltung mit Vergaberechten, oder dem Einsatz von Chipkarten, wie der Thoska. Der Zutritt zu schutzbedürftigen Räumen von nicht autorisiertem Personal (z. B. Besuchern, Wartungspersonal) darf nur bei Anwesenheit oder in Begleitung Zutrittsberechtigter erfolgen.

Bei Abwesenheit der Benutzer sind die Räume in denen sich IT-Systeme befinden verschlossen zu halten. Bei der Anordnung und baulichen Einrichtung der Geräte ist darauf zu achten, dass schützenswerte Daten nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

Brandschutz (M 1.5)

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	Servicezentrum Liegenschaften, Beauftragter für Sicherheitsmanagement

Die bestehenden Brandschutzvorschriften sind unbedingt einzuhalten.
In allen Räumen der Bauhaus-Universität und der Hochschule für Musik FRANZ LISZT besteht Rauchverbot. Brand- und Rauchschutztüren sind stets geschlossen zu halten und dürfen nicht (unzulässig) z. B. durch Keile offen gehalten werden.

Die Fluchtwege müssen immer offen gehalten werden, das heißt insbesondere, dass sie nicht versperrt werden dürfen, z. B. durch im Flur abgestelltes Inventar oder indem die Fluchttüren abgeschlossen werden.

Muss ein Gebäude auf Grund eines Brandes verlassen werden, ist gemäß der Anweisungen im Punkt „Flucht und Rettung“ zu handeln:
http://www.uni-weimar.de/cms/?id=flucht

Beim Einsatz von Handfeuerlöschern sind folgende Informationen zu beachten:
http://www.uni-weimar.de/cms/?id=feuerloescher
Die Beschäftigten sollten sich die Standorte des nächsten Feuerlöschers einprägen.

Sicherung tragbarer IT-Systeme (M 1.6)

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

Bei der Speicherung von schutzbedürftigen Daten auf tragbaren IT-Systemen (Laptops. PDAs, Smartphones etc.) und auf mobilen Datenträgern (z. B. Disketten, CDs, DVDs oder USB-Sticks), die auf Grund ihrer Bauart leicht gestohlen werden können, sind besondere Schutzmaßnahmen (Verschlüsselung) zu treffen, um ein unberechtigtes Auslesen dieser Daten zu verhindern.

Bei kurzen Arbeitsunterbrechungen muss unbedingt ein Zugriffsschutz - wie im Abschnitt Abmelden und ausschalten (M 1.10) beschrieben - aktiviert werden.
Um einen tragbares IT-System vor Diebstahl zu schützen, sollten die Zeiten, in denen das Gerät unbeaufsichtigt bleibt, minimiert werden.

Wird das Gerät in einem Kraftfahrzeug aufbewahrt, sollte es von außen nicht sichtbar sein. Da ein tragbares IT-System besonders leicht zu transportieren und zu verbergen ist, sollte das Gerät außerhalb der Nutzungszeiten weggeschlossen oder angekettet werden.

2. 3 Hard- und Softwareeinsatz

Kontrollierter Softwareeinsatz (M 1.7)

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

Auf Rechnersystemen der Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT darf nur Software aus vertrauenswürdigen Quellen bezogen, installiert und genutzt werden, die von der zuständigen Stelle dafür freigegeben wurde. Das eigenmächtige Einspielen, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn eine Genehmigung der zuständigen Stelle vorliegt oder ein Bereich eine pauschale Freigabe für Teilbereiche festgelegt hat. In diesem Fall gelten alle Regelungen für IT-Personal (s.u.) entsprechend.

Keine private Hard- und Software (M 1.8)

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

Die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT und deren Netzen ist ausschließlich im Bereich der Wohnheime des Studentenwerk Thüringen und öffentlichen VPN Dosen sowie dem WLAN-Netzbereich gestattet. Sondergenehmigungen, zum Beispiel im Rahmen von Schulungsveranstaltungen oder Vorträgen, können auf Antrag durch die zuständigen IT-Verantwortlichen des Bereichs oder dafür zuständiges IT-Personal erteilt werden.

Malwareschutz (M 1.9)

Verantwortlich für Initiierung:	zentraler IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung:	IT-Personal , IT-Anwender

Alle IT-Systeme (auch Testsysteme) sind, soweit technisch möglich, vor Malware (= Schadsoftware, wie Viren, Würmer, Trojanische Pferde, Dialer, Spyware, RootKits etc.) durch aktuelle und ständig aktivierte Schutzprogramme abzusichern. Das SCC stellt unter
https://www.uni-weimar.de/cms/?id=schutz
und
http://www.uni-weimar.de/cms/?id=tools
die entsprechenden Programme bereit.
Alle IT-Systeme der Weimarer Hochschulen sollten, soweit immer möglich, in das zentrale Malwareschutz-Management-System integriert werden.
Beim Verdacht auf Infektion mit Malware ist in jedem Falle das zuständige IT-Personal zu informieren. Neben der Meldung durch Schutzprogramme können unerklärliches Systemverhalten, ungewöhnlich hoher Ressourcenverbrauch oder unerwartete Netz-Zugriffe Anzeichen für einen Malwarebefall sein.

2. 4 Zugriffsschutz

Abmelden und ausschalten (M 1.10)

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

Bei längerer Abwesenheit muss sich der Benutzer aus den laufenden Anwendungen und dem Betriebssystem abmelden. Ist absehbar, dass nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann an Stelle des Abmeldens auch die manuelle Aktivierung der Bildschirmsperre erfolgen, die nur durch eine erfolgreiche Benutzerauthentifizierung, also z. B. eine Passwortabfrage, deaktiviert werden kann. Zusätzlich ist sollte die Bildschirmsperre nach einem vorgegebenen Inaktivitäts-Zeitraum von 10 Minuten automatisch gestartet werden.

Grundsätzlich sind die Systeme nach der Abmeldung auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen.

Personenbezogene Kennungen (M 1.11)

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

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

Gebrauch von Passwörtern (M 1.12)

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

Die geltenden Festlegungen unter:
http://www.uni-weimar.de/cms/?id=passwort sind einzuhalten, insbesondere bei der Wahl eines Passwortes.
Der Benutzer hat sein Passwort geheim zu halten.
Idealerweise sollte das Passwort nicht notiert werden. Das Passwort sollte allenfalls für die Hinterlegung schriftlich fixiert werden, wobei es in diesem Fall in einem verschlossenen Umschlag sicher aufbewahrt werden muss. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren
Zentral vergebene Passwörter müssen umgehend durch individuelle Passwörter ersetzt werden. Das Passwort muss gemäß der geltenden Festlegungen, regelmäßig gewechselt werden.

Erhält ein Benutzer beim Anmelden mit seinem Passwort keinen Zugriff auf das System, besteht die Gefahr, dass sein Passwort durch Ausprobieren ermittelt werden sollte, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem zuständigen Vorgesetzten und dem IT-Personal zu melden. (Siehe M 1.3)

Vergisst ein Benutzer sein Passwort oder hat er den Verdacht, dass eine unautorisierte Person das Passwort kennt hat er beim zuständigen Administrator bzw. der Benutzerverwaltung das Zurücksetzen zu veranlassen.

Zugriffsrechte (M 1.13)

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

Der Benutzer wird vom zuständigen IT-Personal nur mit den Zugriffsrechten auf IT-Anwendungen, Teilanwendungen oder Daten ausgestattet, die für seine Aufgabenwahrnehmung notwendig sind ("Need-to-know-Prinzip"). Die Zugriffsrechte werden in der Regel durch die Rechteverwaltung des IT-Systems umgesetzt.

Netzzugänge (M 1.14)

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

An das Datenkommunikationsnetz Bauhaus-Universität Weimar dürfen nur Computer, Übertragungseinrichtungen und Geräte angeschlossen werden, die vom Betreiber[6] zugelassen sind. Insbesondere die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems, WLAN-Access-Points o. ä.) ist unzulässig.

[6] = Servicezentrum für Computersysteme und -kommunikation

2. 5 Kommunikationssicherheit

Sichere Netzwerknutzung (M 1.15)

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

Der Einsatz von verschlüsselten Kommunikationsdiensten ist, nach Möglichkeit, den unverschlüsselten Diensten vorzuziehen.
Schutzbedürftige Daten sind immer verschlüsselt zu übertragen.

2. 6 Datensicherung

Datensicherung (M 1.16)

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

Regelmäßig durchgeführte Datensicherungen sollen vor Datenverlust schützen. Grundsätzlich sind Daten auf zentralen Servern zu speichern. Ist die Nutzung von zentralen Servern nicht möglich, ist der Benutzer für die Sicherung seiner Daten selbst verantwortlich.
Informationen zum Backup-Service des SCC finden sich unter:
https://www.uni-weimar.de/cms/?id=backup
Vertrauliche Daten sollten vor der Sicherung möglichst verschlüsselt werden, wobei darauf zu achten ist, dass eine Entschlüsselung auch nach einem längeren Zeitraum möglich sein sollte.
Der Ausdruck von Daten auf Papier ist keine angemessene Art der Datensicherung.

2. 7 Umgang mit Datenträgern und schützenswerten Daten

Sichere Aufbewahrung (M 1.17)

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

Mobile Datenträger mit schützenswerten Daten sind so aufzubewahren, dass zum einen ein unbefugter Zugriff durch die Verwendung geeigneter, verschlossener Behältnisse, Schränke, Räume verhindert wird und zum anderen die Lagerungsbedingungen gemäß den Herstellerangaben eingehalten werden. Insbesondere ist darauf zu achten, dass ein hinreichender Schutz gegen Magnetfelder und Staub, sowie eine klimagerechte Lagerung gewährleistet ist.

Datenträgerkennzeichnung (M 1.18)

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

Zur schnellen Identifizierung sind Datenträger soweit möglich eindeutig zu kennzeichnen. Bei schützenswerten Informationen sollte die Kennzeichnung jedoch für Unbefugte keine Rückschlüsse auf den Inhalt erlauben, um einen Missbrauch zu erschweren. Eine festgelegte Struktur von Kennzeichnungsmerkmalen (z. B. Verfahren, Dateien, Inhalt, Datum der ersten Ingebrauchnahme, sowie das Datum des erstmaligen und letztmaligen Beschreibens) erleichtert die Zuordnung in Bestandsverzeichnissen. Darüber hinaus sollten die Datenträger mit den für das Auslesen notwendigen Parametern gekennzeichnet werden.

Gesicherter Transport (M 1.19)

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

Die Übermittlung von Datenträgern mit vertraulichen Daten hat dem Schutzbedarf angemessen zu erfolgen.
Sollen zwischen zwei oder mehreren Kommunikationspartnern Datenträger ausgetauscht werden, so sind zum ordnungsgemäßen Austausch folgende Punkte zu beachten:

- Die Adressierung muss eindeutig erfolgen, um eine fehlerhafte Zustellung zu vermeiden. So sollten neben dem Namen des Empfängers auch Organisationseinheit und die genaue Bezeichnung der Behörde/des Unternehmens angegeben sein. Entsprechendes gilt für die Adresse des Absenders.
- Dem Datenträger sollte (optional) ein Datenträgerbegleitzettel beigelegt werden, der folgende Informationen umfasst: Absender, Empfänger, Art des Datenträgers, Seriennummer (soweit vorhanden), Identifikationsmerkmal für den Inhalt des Datenträgers, Datum des Versandes, ggf. Datum bis wann der Datenträger spätestens den Empfänger erreicht haben muss, Hinweis, dass Datenträger auf Viren überprüft sind, Parameter, die zum Lesen der Informationen benötigt werden, z. B. Bandgeschwindigkeit.
- Jedoch sollte nicht vermerkt werden, welches Passwort für die eventuell geschützten Informationen vergeben wurde, welche Schlüssel ggf. für eine Verschlüsselung der Informationen verwendet wurde, welchen Inhalt der Datenträger hat.
- Der Versand des Datenträgers kann (optional) dokumentiert werden. Für jede stattgefundene Übermittlung ist dann in einem Protokoll festzuhalten, wer wann welche Informationen erhalten hat. Je nach Schutzbedarf beziehungsweise Wichtigkeit der übermittelten Informationen ist der Empfang zu quittieren ein Quittungsvermerk und dem erwähnten Protokoll beizufügen.
- Es sind jeweils Verantwortliche für den Versand und für den Empfang zu benennen.
- Die Versandart ist dem Schutzbedarf abgemessen festzulegen.

Die Versandverpackung ist so zu wählen dass Manipulationen am Datenträger durch Veränderungen an der Verpackung erkennbar sind.
Verfügt der Datenträger über einen Schreibschutz so sollte dieser genutzt werden.

Sollen Manipulationen an den Informationen auf dem Datenträger selbst erkannt werden, sind Verschlüsselungs- oder Checksummen-Verfahren einzusetzen.

Löschen und Entsorgung von vertraulichem Papier und Datenträgern (M 1.20)

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

Maßgeblich ist hier die Richtlinie zur Entsorgung, Veräußerung Ausgabe und Weitergabe von Datenträgern und IT-Geräten an der Bauhaus-Universität Weimar (MdU 27/2008) vom 20.05.2008. Die dort fixierten Maßnahmen sind umzusetzen.

Schützenswerte Daten auf dem Arbeitsplatz-PC (M 1.21)

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

Das Speichern schützenswerter Daten auf der Festplatte des Arbeitsplatz-PCs oder anderer lokaler Speicher- oder Übertragungsmedien und deren Übertragung ist nur verschlüsselt zulässig. Die Zugriffsrechte der verschlüsselten Dateien sind so zu setzen, dass Unbefugte keinen Zugriff erlangen können. (Siehe auch M 1.17)

3. Maßnahmen des IT-Grundschutzes für IT-Personal

Die im Folgenden beschriebenen Maßnahmen richten sich an alle Mitarbeiter der Bau-haus-Universität Weimar und der Hochschule für Musik FRANZ LISZT, 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 Maßnahmen ergänzen die im vorangegangenen Abschnitt dargestellten Maßnahmen für den IT-Anwender, die auch für das IT-Personal maßgeblich sind.

Im Interesse einer möglichst kompakten Darstellung sollen hier nur ergänzende Maßnahmen und Aspekte aufgeführt 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 sind aber die zugrunde liegenden Sicherheitsaspekte nicht außer Kraft zu setzen, sondern der gegebenen Situation anzupassen.

3. 1. Allgemeines

Grundsätze für den IT-Einsatz (M 2.1)

Verantwortlich für Initiierung:	Hochschulleitungen (Fachbeirat SCC)
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 Thüringen zu beachten, die eine ordnungsgemäße IT-Organisation, Verfahrensplanung und -realisierung beschreiben, soweit diese für die Bauhaus-Universität Weimar und die Hochschule für Musik FRANZ LISZT verbindlich sind.
IT-Sicherheitsaspekte sind bereits zu Beginn eines Projektes (z. B. bei der Anschaffung neuer Software oder bei der Planung von Geschäftsprozessen) zu berücksichtigen. Gerade neue Techniken dürfen nicht unkritisch eingesetzt werden.

Gesamtverantwortung (M 2.2)

Verantwortlich für Initiierung:	Hochschulleitungen (Fachbeirat SCC)
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, Zentraleinrichtungen und -instituten und der Zentralen Universitätsverwaltung entsprechend den Regelungen des Thüringer Hochschulgesetzes.

3. 2. Organisation von IT-Sicherheit

Sicherheitsmanagement (M 2.3)

Verantwortlich für Initiierung:	Hochschulleitungen (Fachbeirat SCC)
Verantwortlich für Umsetzung:	Sicherheits-Management-Team (SMT)

Ein gutes IT-Sicherheitsniveau lässt sich nur dann erreichen, wenn Schritt für Schritt die Einrichtung eines umfassenden IT-Sicherheitsmanagements vorgenommen wird. Hierzu wurde durch die Hochschulleitungen die IT-Sicherheitsordnung erlassen:
http://www.uni-weimar.de/cms/?id=sicherheitsordnung
und das IT-Sicherheits-Management-Team eingesetzt:
http://www.uni-weimar.de/cms/?id=smt .

Beschreibung von IT-Verfahren (M 2.4)

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

Der gesamte IT-Einsatz ist in IT-Verfahren zu gruppieren. Jedes Verfahren ist zu beschreiben. Zu den unverzichtbaren Bestandteilen einer Verfahrensbeschreibung gehören:

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

Rollentrennung (M 2.5)

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

Für jedes IT-Verfahren sind die Verantwortlichkeiten für alle Bereiche eindeutig festzulegen. Es sollte eine Rollentrennung von operativen und kontrollierenden Funktionen erfolgen (zum Beispiel Rollentrennung von Systemadministration und Revision). Jedem Mitarbeiter müssen die ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein. Abgrenzungen und Schnittflächen der verschiedenen Anwenderrollen müssen klar definiert sein.

Dokumentation der IT-Verfahren bezüglich der IT-Sicherheit (M 2.6)

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

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

- Vertretungsregelungen, insbesondere im Administrationsbereich
- Zugriffsrechte
- Organisation, Verantwortlichkeit und Durchführung der Datensicherung
- Installation und Freigabe von Software
- Zweck, Freigabe und Einsatz selbsterstellter Programme
- Dienstanweisungen
- Arbeitsanleitungen für Administrationsaufgaben etc.
- auftretende Sicherheitsprobleme aller Art
- Notfallregelungen
- Wartungsvereinbarungen
- Verfahrensbeschreibungen nach Datenschutzrecht

Nur dokumentierte Verfahren dürfen betrieben werden.
Der IT-Verantwortliche sorgt für die aktuelle Dokumentation der Verfahren seines Bereiches.
Der IT-Verantwortliche ist verantwortlich für die Erstellung und Pflege der Dokumentation der IT-Verfahren seines Bereiches.

Dokumentation von sicherheitsrelevanten Ereignissen und Fehlern (M 2.7)

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

Ereignisse, die Indiz für ein Sicherheitsproblem sein können, wie Systemabstürze, Hardwareausfälle sowie das Eindringen Unbefugter, können für die Fortschreibung der IT-Sicherheitsrahmenrichtlinie wertvolle Hinweise liefern. Sie sind daher zu dokumentieren. Die Dokumentationen sicherheitsrelevanter Vorfälle sind an das SMT/ die Operative Gruppe weiterzuleiten, da sie eine wichtige Grundlage für den jährlich zu erstellenden IT-Sicherheitsbericht[7] darstellen. 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. Bei sicherheitsrelevanten Vorfällen, die möglicherweise Straftatbestände berühren, empfiehlt sich die Abstimmung mit dem Justiziar der Hochschule.

[7] Vgl. IT-Sicherheitsordnung für die Hochschule für Musik FRANZ LISZT Weimar und die Bauhaus-Universität Weimar vom 04. Juli 2005

Regelungen der Auftragsdatenverarbeitung (M 2.8)

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

Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag der Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT betriebenen IT-Verfahren. Die Verantwortung für die IT-Sicherheit ist eindeutig zuzuweisen und entsprechende Kontrollmöglichkeiten vorzusehen.
Sofern im Rahmen der Auftragsdatenverarbeitung personenbezogene Daten verarbeitet werden, sind die Regelungen des §8 des Thüringer Datenschutzgesetzes zu beachten.
Die genannten Regelungen Thüringer Datenschutzgesetzes sind ebenfalls bei Wartungsarbeiten anzuwenden, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Standards für technische Ausstattung (M 2.9)

Verantwortlich für Initiierung:	Hochschulleitungen (Fachbeirat SCC)
Verantwortlich für Umsetzung:	IT-Dienstleister

Zur Erreichung eines ausreichenden Sicherheitsniveaus für IT-Systeme sind Qualitätsstandards im Sinne dieses Konzepts von den zentralen Dienstleistern unter Maßgabe der vom Fachbeirat SCC definierten Strategien festzulegen.

Zentralisierung wichtiger Serviceleistungen (M 2.10)

Verantwortlich für Initiierung:	Hochschulleitungen (Fachbeirat SCC)
Verantwortlich für Umsetzung:	IT-Dienstleister

Ein leistungsfähiger Nutzerservice, zentral gesteuerte Datensicherungsmaßnahmen, die Möglichkeit der Ablage von Daten auf zentrale File-Server 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. Malwareschutz und Firewall-Einsatz sind ebenfalls zu zentralisieren.
Beim Einsatz netzwerkweit operierender Installations- und Inventarisierungswerkzeuge sind besondere Maßnahmen zum Schutz vor Missbrauch zu ergreifen. Insbesondere müssen verbindliche Regelungen getroffen werden, die sicherstellen, dass die Werkzeuge ausschließlich für diesen Zweck eingesetzt werden. Dazu muss u. a. festgelegt sein, dass die Werkzeuge nur auf dafür bestimmten, besonders abgesicherten Arbeitsplätzen eingesetzt werden. Der Personenkreis, der berechtigt ist, diese Werkzeuge zu nutzen, ist auf das notwendige Maß zu beschränken. Die Anwender sind vor dem Einsatz solcher Werkzeuge zu informieren. Ihr Einsatz muss protokolliert und dokumentiert werden.

Revision der IT-Sicherheit (M 2.11)

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

Alle eingesetzten IT-Sicherheitsmaßnahmen müssen auf ihre Tauglichkeit, Wirksamkeit und Einhaltung überprüft werden. Diese Überprüfung muss regelmäßig (unangekündigt) und nach jeder Änderung der Sicherheitsstandards erfolgen. Dies kann mit Hilfe entsprechender Tools von den zuständigen IT-Stellen der Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT 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.)
Primäres Ziel der Kontrollen ist es Mängel festzustellen, ihre Ursachen zu ermitteln und Lösungen aufzuzeigen, beispielsweise durch die Änderung bestehender Regelungen oder die Hinzunahme technischer Maßnahmen.

3. 3. Personelle Maßnahmen

Zahlreiche Untersuchungen und Statistiken über Fehlfunktionen im IT-Bereich zeigen, dass die größten Risiken durch fehlende bzw. unzureichende Kenntnisse, Nachlässigkeit, mangelndes Sicherheitsbewusstsein, und Überforderung der Mitarbeiter entstehen. Daher sind die in diesem Abschnitt aufgeführten Maßnahmen vorrangig zu beachten.

Sorgfältige Personalauswahl (M 2.12)

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	Bereichsleitung

Mit Administrationsaufgaben auf Netzwerk- und Systemebene dürfen nur sorgfältig ausgewählte, ausreichend qualifizierte, vertrauenswürdige, zuverlässige und motivierte Mitarbeiter betraut werden. Kurzzeitig befristet beschäftigte Mitarbeiter (Beschäftigungsverhältnis von weniger als einem Jahr) sollten nach Möglichkeit keine Aufgaben übernehmen, die nur mit Administratorrechten ausgeführt werden können.
Das eingesetzte Personal ist regelmäßig darüber zu belehren, dass die Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen.

Angemessene Personalausstattung (M 2.13)

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

Eine zuverlässige und sichere Erfüllung der IT-Aufgaben erfordert eine angemessene Personalausstattung. Dabei spielen System- und Netzwerkadministratoren eine besondere Rolle.

Vertretung (M 2.14)

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

Vertretungsregelungen haben den Sinn, für vorhersehbare (Urlaub, Dienstreise) und auch unvorhersehbare Fälle (Krankheit, Unfall, Kündigung) des Personalausfalls die Fortführung der Aufgabenwahrnehmung zu ermöglichen.

Da dem Administrator hinsichtlich der Funktionsfähigkeit der eingesetzten Hard- und Software eine Schlüsselrolle zukommt, muss auch bei seinem Ausfall die Weiterführung seiner Tätigkeiten gewährleistet sein. Hierzu müssen die benannten Vertreter über die erforderlichen Kenntnisse und Befähigungen verfügen, den aktuellen Stand der Systemkonfiguration kennen, sowie im Bedarfsfall sofort (aber auch erst dann) Zugriff auf die für die Administration benötigten Zutritts-, Zugangs- und Zugriffsberechtigungen haben.
Die Übernahme von Aufgaben im Vertretungsfall setzt voraus, dass der Verfahrens- oder Projektstand hinreichend dokumentiert ist.
Die durch den Vertreter zu erledigenden Aufgaben und die ihm eingeräumten Kompetenzen müssen klar festgelegt sein.

Qualifizierung (M 2.15)

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

(Siehe auch Abschnitt Anwenderqualifizierung (M 1.1))
IT-Personal darf erst nach ausreichender Schulung mit IT-Verfahren arbeiten. Es muss sichergestellt sein, dass die ständige Fortbildung des IT-Personals in allen ihr Aufgabengebiet betreffenden Belangen erfolgt.

3. 4. Sicherung der Infrastruktur

Sicherung der Serverräume (M 2.16)

Verantwortlich für Initiierung:	IT-Verantwortlicher
Verantwortlich für Umsetzung:	Servicezentrum Liegenschaften/ IT-Personal

Alle IT-Systeme mit typischer Serverfunktion, einschließlich der Peripheriegeräte (Konsolen, externe Platten, Laufwerke u. ä.), sind in separaten, besonders gesicherten Räumen aufzustellen. Für die in Serverräumen betriebenen IT-Systeme wird in vielen Fällen ein hohes Maß an Verfügbarkeit gefordert. Diesen Anforderungen ist durch redundante Auslegung der infrastrukturellen und technischen Einrichtungen Rechnung zu tragen.
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 und technische Härtungsmaßnahmen, wie zum Beispiel spezielle Wand-, Tür- und Fensterkonstruktionen und

die Verwendung von Gefahrenmeldern o. ä. zur Verhinderung oder zumindest zum Anzeigen eines gewaltsamen Eindringens vorzusehen. Serverräume, in denen besonders schützenswerte Daten gespeichert bzw. verarbeitet werden und die nicht über entsprechende bauliche Sicherungsvorkehrungen verfügen, sollen möglichst unauffällig sein, d. h. Hinweisschilder u. ä. sollten nicht angebracht werden, damit die Funktion der Räume nicht sofort erkennbar wird. Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; verwendete Schlüssel müssen kopiergeschützt sein. Für die Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen.
Der Zutritt muss auf diejenigen Personen begrenzt werden, deren Arbeitsaufgaben dieses erfordert. Die Personen sollten gegenseitig ihre Berechtigungen kennen, um Unberechtigte als solche identifizieren zu können. Der Zutritt zu Serverräumen von nicht autorisiertem Personal (z. B. Besuchern, Reinigungs- und Wartungspersonal) darf nur bei Anwesenheit oder in Begleitung Zutrittsberechtigter erfolgen.
In einem Serverraum sollten sich auf keinen Fall Geräte oder Ausrüstung befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen, also z. B. Fax-Geräte oder Fotokopierer. Brennbare Materialen sollten ebenfalls nicht in einem Serverraum gelagert werden.

Geeignete Aufstellung eines IT-Systems (M 2.17)

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

(Siehe auch Abschnitt Räumlicher Zugangsschutz (M 1.4))
Hinsichtlich der Schlüsselverwaltung muss gewährleistet sein, dass Schlüssel nur an die jeweils berechtigten Personen ausgegeben werden.
Bei der Aufstellung eines IT-Systems sollten verschiedene Voraussetzungen beachtet werden, die die Lebensdauer und Zuverlässigkeit der Technik verbessern und die Ergonomie berücksichtigen. Einige seien hier genannt:

- ein IT-System ist nicht in unmittelbarer Nähe der Heizung aufzustellen, um eine Überhitzung zu vermeiden,
- ein IT-System ist nicht der direkten Sonneneinstrahlung auszusetzen,
- Staub und Verschmutzungen sind zu vermeiden, da die mechanischen Bauteile beeinträchtigt werden können,
- direkte Lichteinstrahlung auf den Bildschirm ist aus ergonomischen Gründen zu vermeiden,
- der Standort ist so zu wählen, dass die Möglichkeit des Beobachtens von außerhalb minimiert wird.

Sicherung der Netzknoten (M 2.18)

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

Vernetzungsinfrastruktur (Switches, Router, Hubs 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 (M 2.17).

Verkabelung und Funknetze (M 2.19)

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

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

Trassen-Sicherung und Auswahl geeigneter Kabeltypen (M 2.20)

Verantwortlich für Initiierung:	Hochschulleitungen (Fachbeirat SCC)
Verantwortlich für Umsetzung:	IT-Dienstleister

Kabeltrassen sind so zu führen und zu dimensionieren, dass mögliche Gefährdungen minimiert werden. Neben der Verhinderung des Zugriffs durch Unbefugte, ist ein Schutz vor Beschädigungen, Umwelteinflüssen und Bränden zu realisieren. Hierbei spielt auch die Auswahl geeigneter Kabeltypen gemäß den übertragungstechnischen Notwendigkeiten und unter Beachtung der jeweiligen Verlege- bzw. Umfeld-Bedingungen eine entscheidende Rolle.

Einweisung und Beaufsichtigung von Fremdpersonal (M 2.21)

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

Fremde Personen, die in gesicherten Räumen mit IT (z.B. Serverräume) Arbeiten auszuführen haben, müssen beaufsichtigt werden. Personen, die nicht unmittelbar zum IT-Bereich zu zählen sind, aber Zugang zu gesicherten IT-Räumen benötigen, müssen über den Umgang mit IT belehrt werden bzw. ihnen ist eine unautorisierte Nutzung explizit zu untersagten.
Wenn bei Arbeiten durch externe Firmen, zum Beispiel im Rahmen der Fernwartung, die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, ist gemäß §8 Abs. 7 die Einhaltung der Bestimmungen des §8 Abs. 1 bis 5 ThürDSG zu fordern.

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

Gesicherte Stromversorgung und Überspannungsschutz (M 2.22)

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

Alle wichtigen IT-Systeme dürfen nur an eine ausreichend dimensionierte und gegen Überspannungen abgesicherte Stromversorgung angeschlossen werden. Die Stromversorgung ist wenn möglich redundant auszulegen. Eine entsprechende Versorgung ist in Zusammenarbeit mit dem Servicezentrum Liegenschaften herzustellen. Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und ggf. ersetzt werden. Insbesondere bei Neugestaltung eines Schutzkonzeptes für Überspannung sind Auslegung und Funktionsweise bestehender USV (unterbrechungsfreier Stromversorgung) und NEA (Netzersatzanlage) zu berücksichtigen.

Unterbrechungsfreie Stromversorgung (M 2.23)

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), IT-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) anzuschließen, um Totalausfälle der Stromversorgung und Unterspannungen zu überbrücken und Überspannungen zu glätten..Die Konfiguration der USV und der durch sie geschützten Systeme muss ein rechtzeitiges und geordnetes Herunterfahren der Systeme gewährleisten. Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der USV vorzusehen.

Aus Gründen des Brandschutzes[8] sollten zentrale USV-Systeme möglichst räumlich getrennt von den zu versorgenden und anderen IT-Systemen aufgestellt werden.

[8] Gemäß TELA-Versicherung sind USVs in 50% aller Brände, die in Rechnerräumen entstehen, ursächlich.

Brandschutz (M 2.24)

Verantwortlich für Initiierung:	IT-Verantwortlicher IT-Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Servicezentrum Liegenschaften, Beauftragter für Sicherheitsmanagement

(Siehe auch Abschnitt Brandschutz (M 1.5)).
Insbesondere in Räumen mit wichtiger Informationstechnik, wie beispielsweise Serverräumen, sind die Brandlasten zu minimieren. Verbrauchsmaterial, leere Verpackungen und andere leicht entflammbare Materialen dürfen in diesen Räumen nicht gelagert werden. Die Türen zu diesen Räumen sollen brandhemmend ausgelegt sein.
Außerdem sind Brandmelder und Handfeuerlöscher (Brandklasse B mit Löschgas) vorzusehen. Die Feuerlöscher müssen regelmäßig geprüft und gewartet werden. Die Feuerlöscher müssen so angebracht werden, dass sie im Brandfall leicht erreichbar sind.
Es sollte regelmäßig eine Brandschutzbegehung und gelegentlich eine Brandschutzübung stattfinden, bei der die Mitarbeiter auch in die Benutzung der Handfeuerlöscher einzuweisen sind.

Schutz vor Wasserschäden (M 2.25)

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), IT-Verfahrensverantwortlicher (verfahrensspezifisch)
Verantwortlich für Umsetzung:	Servicezentrum Liegenschaften, Beauftragter für Sicherheitsmanagement

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. Damit eingetretenes Wasser schnellstmöglich wieder aus dem Bereich der IT-Systeme entfernt werden kann, sind ausreichend dimensionierte Abflüsse mit Rückschlagventilen und wenn nötig Pumpen vorzusehen. Zusätzlich kann in besonders kritischen Bereichen auch der Einsatz von Wassermeldeanlagen sinnvoll sein. Es ist regelmäßig eine Prüfung der Funktionstüchtigkeit durchzuführen.

Klimatisierung (M 2.26)

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

Um den zulässigen Betriebstemperaturbereich von IT-Geräten zu gewährleisten, reicht der normale Luft- und Wärmeaustausch eines Raumes manchmal nicht aus, so dass der Einbau einer Klimatisierung erforderlich ist (z.B. wie beim Server-Raum im SCC).
Um die Schutzwirkung aufrechtzuerhalten, ist eine regelmäßige Wartung der Klimatisierungseinrichtung vorzusehen. Eine zusätzliche Überwachungseinrichtung für die Klimatisierung ist vorzusehen, insbesondere bei Vollklimatisierung.

Da bei einem Ausfall der Klimatisierung unter Umständen viele (insbesondere wichtige) IT-Systeme abgeschaltet werden müssen, sollte diese auf eine hohe Verfügbarkeit ausgelegt sein.

3. 5. Hard- und Softwareeinsatz

Beschaffung, Softwareentwicklung (M 2.27)

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 Bereichen durchgeführt.

Kontrollierter Softwareeinsatz (M 2.28)

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

(Siehe auch Abschnitt Kontrollierter Softwareeinsatz (M 1.7))
Bei der Freigabe von Software muss darauf geachtet werden, dass die Software aus zuverlässiger Quelle stammt und dass ihr Einsatz notwendig ist.

Separate Entwicklungsumgebung (M 2.29)

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

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

Test von Software (M 2.30)

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

Vor dem Einsatz neuer Hardware-Komponenten oder neuer Software/ Versionen müssen diese auf speziellen Testsystemen hinreichend geprüft werden. Neben der Lauffähigkeit des Produktes ist dabei insbesondere zu überprüfen, dass der Einsatz neuer Komponenten keine negativen Auswirkungen auf die laufenden IT-Systeme hat. Da vor erfolgreichen Tests Schadfunktionen nicht ausgeschlossen werden können und da bei Tests Fehler provoziert werden, sind immer vom Produktionsbetrieb isolierte Testsysteme zu verwenden.
Der Testverlauf und das Testergebnis sind zu dokumentieren.

Erst nach bestandenem Test dürfen neue Komponenten für die Installation auf Produktionssystemen freigegeben werden.

Entwicklung von Software nach standardisierten Verfahren (M 2.31)

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

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

Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates (M 2.32)

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

Um entdeckte Schwachstellen in Software-Produkten und bestimmten Hardware-Komponenten schnellst möglich zu beheben, damit sie nicht durch potentielle Angreifer ausgenutzt werden können ist es unabdingbar, dass Patches und Updates der Hersteller zeitnah eingespielt werden. Neben dem Betriebssystem sind auch die eingesetzten Applikationen (einschließlich ihrer Erweiterungen) und Treiber stets aktuell zu halten. Die Software sollte durch automatische Update-Services oder den regelmäßigen Besuch der Hersteller-Webseiten immer auf dem aktuellen Stand gehalten werden.

Systemadministratoren sollten sich daher regelmäßig über bekannt gewordene Software-Schwachstellen informieren.

Die Integrität und Authentizität der einzuspielenden Sicherheitsupdates und Patches ist sicherzustellen (Nutzung vertrauenswürdigen Quellen), außerdem sind sie immer mit Hilfe eines Malwareschutzprogramms zu prüfen.

Malwareschutz (M 2.33)

Verantwortlich für Initiierung:	IT-Verantwortlicher, Zentraler IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung:	IT-Personal

(Siehe auch Abschnitt Malwareschutz (M 1.9))
Das IT-Personal hat im eigenen Verantwortungsbereich dafür Sorge zu tragen, dass die im Abschnitt (M 1.9) beschriebenen Maßnahmen umgesetzt werden.
Sollte durch Nutzer der Verdacht des Malwarebefalls gemeldet werden, sind durch einen Administrator die betroffenen Systeme zu ermitteln, weitere Ausbreitung zu verhindern und die Systeme in einen betriebsbereiten Zustand zurückzuversetzen.
Nachdem alle Schadprogramme entfernt worden sind, müssen alle von diesem Rechner aus genutzten Zugangskennungen und Passwörter geändert werden, um einem möglichen Missbrauch vorzubeugen.

Dokumentation (M 2.34)

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), IT-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.
Dokumentationen sind regelmäßig zu aktualisieren. Gut dokumentierte IT-Systeme erleichtern Administrationsarbeiten, die Planung und Neuinstallation von Software, ebenso wie die Fehlerbeseitigung.

Ausfallsicherheit (M 2.35)

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

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

Einsatz von Diebstahl-Sicherungen (M 2.36)

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

Mechanische oder elektronische 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, wie etwa bei Laptops im mobilen Einsatz.
Diebstahl-Sicherungen sind z.B. dort sinnvoll, 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.

3. 6. Zugriffsschutz

(Siehe auch Abschnitt 1.4 Zugriffsschutz)
Grundsätzlich gilt, dass nur die Personen Zugang zu dem Netz und die damit verfügbaren Ressourcen der Bauhaus-Universität Weimar oder der Hochschule für Musik FRANZ LISZT 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.
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 IT-System der Hochschule eine besondere Bedeutung.

Personenbezogene Kennungen (Authentisierung) (M 2.37)

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

(Siehe auch Abschnitt Personenbezogene Kennungen (M 1.11))
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.

Administrative Accounts (M 2.38)

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

Das Verwenden von Benutzerkennungen/ Accounts mit weit reichenden Administrationsrechten muss auf die dafür notwendigen Aufgaben beschränkt bleiben. Die Administratoren erhalten für diese Aufgaben eine persönliche Administratorkennung.
Im Normalfall sollten auch Administratoren lediglich mit eingeschränkten Rechten und nicht mit Administratorrechten arbeiten. Standard Administrator-Konten des Betriebssystems sind nach Möglichkeit umzubenennen, damit deren Bedeutung nicht sofort ersichtlich ist.

Ausscheiden von Mitarbeitern (M 2.39)

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

Verlässt ein Mitarbeiter die Institution, wechselt die Funktion oder ändert sich sein Tätigkeitsfeld, ist einerseits eine Übertragung sicherheitsrelevanter Aufgaben und Funktionen erforderlich, andererseits ist der Entzug der durch Wissen und Besitz dem ehemaligen Mitarbeiter eingeräumten Zutritts-, Zugangs- und Zugriffsrechte für IT-Systeme, IT-Verfahren oder Daten notwendig.
Im organisatorischen Ablauf muss zuverlässig verankert sein, dass der zuständige IT-Verantwortliche rechtzeitig über das Ausscheiden oder den Wechsel eines Mitarbeiters

informiert wird. Der zuständige Bereich des betreffenden Mitarbeiters hat über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung des ausscheidenden Mitarbeiters zugeordnet sind.
Die Weiterführung der übertragenen sicherheitsrelevanten Aufgaben und Funktionen muss auch nach dem Ausscheiden weiter gewährleistet bleiben. Vor dem Weggang ist eine rechtzeitige Einweisung des Nachfolgers durchzuführen. Dafür ist es wünschenswert, dass sich die Arbeitszeiträume wenigstens kurz überschneiden. Vor der Verabschiedung sollte noch einmal explizit darauf hingewiesen werden, dass alle Verschwiegenheitserklärungen weiterhin in Kraft bleiben und keine während der Arbeit erhaltenen Informationen weitergegeben werden dürfen.
Ist die ausscheidende Person ein Funktionsträger in einem Notfallplan, so ist der Notfallplan zu aktualisieren. Die bestehenden Vertreterregelungen sind ebenfalls zu überprüfen und ggf. zu aktualisieren.

Gebrauch von Passwörtern (M 2.40)

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

(Siehe auch Abschnitt Gebrauch von Passwörtern (M 1.12)[9])
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.
Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr gebraucht werden
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen umgehend durch individuelle Passwörter ersetzt werden.
- Die Wahl von Trivialpasswörtern ("BBBBBB", "123456") sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Nach dreifacher fehlerhafter Passworteingabe muss eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Passwörter sollten in Netzen nicht unverschlüsselt übertragen 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.

[9] Es gelten die Festlegungen unter: http://www.uni-weimar.de/cms/?id=passwort. Administratoren haben zusätzlich folgende Regeln zu beachten: http://www.uni-weimar.de/cms/?id=admins

Zugriffsrechte [Autorisierung] (M 2.41)

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

(Siehe auch Abschnitt Zugriffsrechte (M 1.13))
Bei der Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer sind die in den Bereichen geltenden Regelungen zu beachten.
Zugriffsrechte sind restriktiv zu vergeben. Für Benutzer mit besonderen Rechten, insbesondere für Administratorkennungen, ist eine Zugangsbegrenzung auf die notwendigen Rechner (i.d.R. sind es der betreffende Server und die Arbeitsplatz-PCs) zu begrenzen. Es ist ebenfalls zu prüfen, inwieweit die Zugangserlaubnis auf bestimmte Zeiten begrenzt werden kann. Beispielsweise könnte der Zugang zu wichtigen Systemen für die Anwender auf die üblichen Arbeitszeiten eingeschränkt werden.
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.
Die Festlegung und Veränderung von Zugriffsrechten ist vom jeweils Verantwortlichen zu veranlassen und zu dokumentieren.

Abmelden und ausschalten (M 2.42)

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

(Siehe auch Abschnitt Abmelden und ausschalten (M 1.10))
Soweit es technisch möglich ist, sind zentral administrierte IT-Systeme so zu konfigurieren, dass die Maßnahmen im Abschnitt Abmelden und ausschalten (M 1.10), umgesetzt werden und durch den Benutzer nicht ohne weiteres deaktiviert werden können.

3. 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 (§ 9 Abs. 2 Nr. 5 ThürDSG).
Je nach Schutzbedarf des Verfahrens müssen adäquate Maßnahmen zur Protokollierung getroffen werden, um die Revisionsfähigkeit zu gewährleisten. Die hier skizzierten technischen und organisatorischen Lösungen werden in einem gesonderten IT-Revisionskonzept beschrieben.

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 (M 2.43)

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

Protokollierung ist in einem sinnvollen Umfang zu aktivieren. In regelmäßigen Abständen muss der Administrator die Protokolldateien überprüfen. Es muss 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. Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden.
Da Protokolldateien in den meisten Fällen personenbezogene Daten beinhalten, ist das Prinzip der Zweckbindung gemäß § 20 (4) ThürDSG und der Anspruch auf Löschung gemäß § 16 (1) ThürDSG unbedingt einzuhalten.

Protokollierung der Administrationstätigkeit (M 2.44)

Verantwortlich für Initiierung:	IT-Verantwortlicher (bereichsspezifisch), IT-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.

3. 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-Benutzer der Hochschulen sind über die besonderen Risiken und Gefahren der elektronischen Kommunikation und der Datenübermittlung in Kenntnis zu setzen.

Sichere Netzwerkadministration (M 2.45)

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

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

Netzmonitoring (M 2.46)

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

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

Deaktivierung nicht benötigter Netzwerkzugänge (M 2.47)

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 Bauhaus-Universität Weimar verhindert wird.

Kommunikation zwischen unterschiedlichen Sicherheitsniveaus (M 2.48)

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 Bauhaus-Universität Weimar und der Hochschule für Musik FRANZ LISZT sind nicht gestattet.
Falls auf Grund besonderer Umstände die Installation anderer Kommunikationswege unumgänglich ist (z.B. der Betrieb eines Modems zu Fernwartungszwecken), muss dies zuvor durch das Servicezentrum für Computersysteme und -kommunikation genehmigt werden.

3. 9. Datensicherung

Organisation der Datensicherung (M 2.49)

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

(Siehe auch Abschnitt Datensicherung (M 1.16))
Die Datensicherung muss nach einem dokumentierten Datensicherungskonzept erfolgen, das dem Schutzbedarf der zu sichernden Daten angemessen ist. Es muss auch darüber Auskunft geben, nach welchen Kriterien die Datensicherung der Daten erfolgt.
Im Falle personenbezogener Daten sind die geforderten Mindest- bzw. Höchstzeiträume zu beachten.
Das Datensicherungskonzept umfasst alle Regelungen der Datensicherung (was wird von wem nach welcher Methode, wann, wie oft und wo gesichert).

Ebenso ist die Aufbewahrung der Sicherungsmedien zu regeln. Alle Sicherungen und das Aufbewahren von Sicherungsmedien sind zu dokumentieren. (Datum, Art der Durchführung der Sicherung/gewählte Parameter, Beschriftung der Datenträger, Ort der Aufbewahrung)

Anwenderinformation zur Datensicherung (M 2.50)

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

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

Durchführung der Datensicherung (M 2.51)

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

Vorzugsweise sollten Daten auf zentralen File-Servern gespeichert werden. Dort erfolgt turnusmäßig eine zentrale Datensicherung. Wo ein Zugriff auf einen File-Server nicht möglich ist, müssen die Daten lokal gesichert werden.
Sicherungsbänder sind an einem sicheren Ort und nicht in unmittelbarer Nähe des gesicherten IT-Systems zu lagern.
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.
Nach Möglichkeit sind die Konfigurationen aller aktiven Netzkomponenten in eine regelmäßige Datensicherung einzubeziehen.

Verifizierung der Datensicherung (M 2.52)

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

Die Konsistenz der Datensicherungsläufe ist sicher zu stellen, d.h. die Lesbarkeit der Datensicherung ist regelmäßig zu überprüfen. Die Rücksicherung von Backups soll wenigstens einmal jährlich geprüft und geübt werden.

3. 10. Umgang mit Datenträgern und schützenswerten Daten

Sichere Aufbewahrung (M 2.53)

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

(Siehe auch Abschnitt Sichere Aufbewahrung (M 1.17))
Datensicherungs-Datenträger unterliegen 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.
- Für den Katastrophenfall müssen die Backup-Datenträger räumlich getrennt vom gesicherten IT-System aufbewahrt werden, wenn möglich in einem anderen Brandabschnitt.

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

Datenträgerkennzeichnung und -inventarisierung (M 2.54)

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

(Siehe auch Abschnitt Datenträgerkennzeichnung M 1.18))
Für jedes IT-Verfahren ist ein Bestandsverzeichnis aller verwendeten Datenträger zu führen. Dieses Verzeichnis muss stets aktuell gehalten werden.

Weitergabe von Datenträgern (M 2.55)

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

(Siehe auch Abschnitt Gesicherter Transport (M 1.19))
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.