IT-Richtlinie der Humboldt-Universität zu Berlin

- Entwurf, 7.2.2012 –

1. Gegenstand und Geltungsbereich

Der Universitätsbetrieb erfordert in hohem Maß die abgestimmte Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Informationstechnologie (IT) stützen. Funktionierende und sichere IT-Prozesse sind daher eine zentrale Grundlage für die Leistungsfähigkeit der Humboldt-Universität zu Berlin (HU) in Forschung, Studium, Lehre und Verwaltung.

Diese IT-Richtlinie regelt die Zuständigkeiten, die Verantwortungsstrukturen, die Aufgabenzuordnung und die Zusammenarbeit bezüglich der IT-Infrastruktur[1] und der sie betreibenden Institutionen bzw. Personen der Humboldt-Universität. Sie soll den effizienten Einsatz der IT und vor allem die Sicherheit der IT-Infrastruktur, der IT-Prozesse und der Daten bestmöglich fördern.

Die IT-Richtlinie gilt für alle Einrichtungen[2] der Humboldt-Universität, mit Ausnahme der Charité. Sie ist verbindlich für alle Einrichtungen und Personen, die an der HU IT-Dienstleistungen erbringen (IT-Betreiber) oder benutzen (IT-Anwender) und umfasst die gesamte IT-Infrastruktur der HU, einschließlich aller darin betriebenen Hard- und Softwaresysteme.

[1] Gesamtheit der Rechnernetze, Computerhardware, Computersoftware, IT-Anwendungssysteme und Peripherie, die an der HU zum Einsatz gebracht werden – darunter auch mobile Computer einschließlich Smartphones, vernetzte Computer in Steuerungs- und Regelungssystemen (embedded systems) sowie virtualisierte Systeme

[2] z. B. Fakultäten, Institute, Zentralinstitute, Graduate Schools, Interdisziplinäre Zentren, Integrative Forschungsinstitute, Zentraleinrichtungen, Universitätsverwaltung

2. IT-Organisationsstruktur

Die IT-Organisationsstruktur der HU unterscheidet folgende Gremien, Einrichtungen bzw. Personen:

- Leitungsgruppe Informationsprozesse (LGI)
- Medienkommission des Akademischen Senats
- IT-Sicherheitsbeauftragte(r) der HU
- IT-Betreiber
- Leiterinnen und Leiter der Einrichtungen
- DV-Beauftragte der Einrichtungen
- Dezentrale IT-Sicherheitsbeauftragte
- IT-Systemverantwortliche, IT-Systemadministratoren
- IT-Benutzerinnen und –Benutzer
- Behördliche(r) Datenschutzbeauftragte(r)
- Personalvertretungen

Es bestehen folgende IT-spezifische Zuständigkeiten:

(1) **Leitungsgruppe Informationsprozesse (LGI)**

Die LGI wird durch die Präsidentin oder den Präsidenten der HU eingesetzt. Sie verantwortet die Strategie, die Entwicklung und die Kontrolle grundlegender und einrichtungsübergreifender Informationsprozesse der HU und dabei insbesondere auch die Rahmenbedingungen der IT-Sicherheit. Zu Ihren Aufgaben gehören:

- strategische Entscheidungen zur Gestaltung der Informationsinfrastruktur der HU
- die grundlegende Koordination der Beschaffung, Speicherung, Erschließung, Aufbewahrung, des Flusses und des Wiederauffindens von Informationen
- richtungweisende Entscheidungen zur Verteilung und zum Einsatz finanzieller und personeller Ressourcen bezogen auf die Informationsprozesse der HU
- die Bestimmung der bzw. des IT-Sicherheitsbeauftragten der HU

Die LGI setzt die oder den IT-Sicherheitsbeauftragten der HU ein. Sie bezieht die Medienkommission des Akademischen Senats im Sinne der akademischen Selbstverwaltung informativ in Prozesse der Planung und Organisation der IT an der HU ein.

(2) **Medienkommission des Akademischen Senats**

Als Ständige Kommission des Akademischen Senats unterstützt die Medienkommission das Präsidium der HU und die LGI auch in Angelegenheiten, die diese Richtlinie regelt.

(3) **IT-Sicherheitsbeauftragte(r) der HU**

Die oder der hauptamtliche IT-Sicherheitsbeauftragte der HU koordiniert die Maßnahmen zur IT-Sicherheit innerhalb der HU. Zu den Aufgaben gehören:

- Beratung zu hochschulinternen technischen Standards, Richtlinien und Notfallplänen zur IT-Sicherheit und Kontrolle ihrer Umsetzung und Einhaltung im Auftrag der LGI
- Koordinierung sicherheitsrelevanter IT-Projekte
- Auswertung von Problemen und Vorfällen hinsichtlich der IT-Sicherheit, Abstimmung von Gegenmaßnahmen mit den IT-Betreibern

- Koordinierung und Unterstützung der IT-Sicherheitsbeauftragten der Einrichtungen bei ihren Aufgaben und bei ihrer Weiterbildung
- Information der LGI über besondere Probleme und Vorfälle hinsichtlich der IT-Sicherheit an der HU, Abstimmung von Maßnahmen, Erstellung eines jährlichen IT-Sicherheitsberichts

Die oder der IT-Sicherheitsbeauftragte der HU ist einer Vizepräsidentin oder einem Vizepräsidenten der HU direkt unterstellt. Sie oder er sollte kein Leiter einer Einrichtung der HU sein.

(4) **IT-Betreiber**

Der CMS ist als zentraler IT-Betreiber der HU vor allem für die Versorgung aller Einrichtungen der HU mit solchen IT-Dienstleistungen zuständig, die allgemein nutzbar sind und einen einrichtungsübergreifenden Charakter haben.

Dezentrale IT-Betreiber sind Arbeitsgruppen oder Personen in den Einrichtungen der HU, die mit ihren IT-Systemen vorrangig einrichtungsspezifische Dienste erbringen.

Externe IT-Betreiber erbringen für die HU ggf. IT-Dienstleistungen, die vom CMS oder von dezentralen IT-Betreibern in Absprache mit dem CMS beauftragt werden.

Der CMS ist als Betreiber der aktiven Netzkomponenten und der Datenleitungen des Netzes der HU für die Gewährleistung der allgemeinen Netzsicherheit verantwortlich. Wenn für Teilnetze eine erhöhte Netzsicherheit erforderlich ist, sind durch die betroffenen Einrichtungen in Abstimmung mit dem CMS Maßnahmen für die zusätzliche Absicherung dieser Teilnetze zu treffen.

Um akute Gefahren für die IT-Sicherheit im Netz der HU abzuwehren, treffen der CMS bzw. dezentrale IT-Betreiber im Rahmen ihrer Zuständigkeit erforderliche Maßnahmen zur Gefahrenintervention wie z. B. die Sperrung von Netzanschlüssen, von kompromittierten Benutzerkonten bzw. IT-Systemen[3]. Betroffene Leiterinnen und Leiter, Betreiber, Benutzerinnen und Benutzer sowie die zuständigen IT-Sicherheits-beauftragten sind umgehend zu informieren.

Der CMS und die dezentralen IT-Betreiber unterstützen die Tätigkeit der IT-Sicherheitsbeauftragten, der DV-Beauftragten und der IT-Systemverantwortlichen. Der CMS und die dezentralen IT-Betreiber stimmen sich untereinander ab.

Werden externe IT-Dienstleister beauftragt, so ist der Auftraggeber dafür verantwortlich, dass der externe Dienstleister die im Netz der HU geltenden Regelungen einhält.

(5) **Leiterinnen und Leiter der Einrichtungen**

Die Leiterinnen und Leiter der Einrichtungen sind für die Planung und den Einsatz der IT und für die Gewährleistung und Weiterentwicklung der IT-Sicherheit in ihren Einrichtungen verantwortlich. Sie bzw. das von Ihnen beauftragte Personal veranlassen und kontrollieren Maßnahmen in ihrer Einrichtung für die Gewährleistung der Sicherheit von Arbeitsplatzrechnern und der unter ihrer Verantwortung betriebenen IT-Systeme

[3] IT-Systeme im Sinne dieser Richtlinie sind Hardware und/oder Software, IT-Verfahren und IT-Anwendungen, die IT-Dienste anbieten. Beispiele sind: Datennetze, Speichernetze, Server, Client-Server-Systeme, IT-Anwendungen in Einrichtungen der HU

sowie zur Absicherung von Netzbereichen ihrer Einrichtungen, in denen IT-Systeme mit erhöhtem Schutzbedarf betrieben werden.

Die Leiterinnen und Leiter der Einrichtungen sind für die Umsetzung der in dieser Richtlinie aufgeführten Maßnahmen verantwortlich. Sie benennen, beauftragen und koordinieren DV-Beauftragte und IT-Sicherheitsbeauftragte für ihre Einrichtungen und IT-Systemverantwortliche für alle in der Einrichtung betriebenen IT-Systeme.[4]

(6) **DV-Beauftragte**

DV-Beauftragte haben im ihnen zugeordneten Verantwortungsbereich insbesondere folgende Aufgaben:

- Koordinierung und Beratung bezüglich der Planung, der Beschaffung und des Betriebes von IT-Systemen einschließlich der einschlägigen Haushaltstitel
- Ansprechpartner des CMS zur Abstimmung der IT-Dienste der Einrichtung mit den vom CMS angebotenen Diensten und zur Koordinierung von einrichtungsübergreifenden Aspekten der IT
- Information zur ordnungsgemäßen Nutzung von Datennetzen, Hardware und Software gegenüber dem Personal der Einrichtung und den Studierenden
- Koordinierung der Anbindung der lokalen Netze in das Universitätsrechnernetz
- Koordinierung der IT-Systemverantwortlichen der Einrichtung

(7) **Dezentrale IT-Sicherheitsbeauftragte**

Dezentrale IT-Sicherheitsbeauftragte haben im ihnen zugeordneten Verantwortungsbereich insbesondere folgende Aufgaben:

- Konzipierung von Maßnahmen zur Gewährleistung und Weiterentwicklung der IT-Sicherheit der Einrichtung im Auftrag der Leitung der jeweiligen Einrichtung, Kontrolle der Umsetzung
- Ansprechpartner des CMS und der oder des Sicherheitsbeauftragten der HU hinsichtlich der IT-Sicherheit
- Meldung sicherheitsrelevanter Vorfälle und der Maßnahmen zu ihrer Behebung an die IT-Sicherheitsbeauftragte oder den IT-Sicherheitsbeauftragten der HU, den CMS und an die Leitung der Einrichtung
- Initiierung und Prüfung von Sicherheitskonzepten für IT-Systeme in ihrem Verantwortungsbereich
- Koordinierung der Schulung des IT-Personals und der IT-Benutzerinnen und -Benutzer hinsichtlich der IT-Sicherheit

Die IT-Sicherheitsbeauftragten sind verpflichtet, sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf dem aktuellen Stand zu halten. Sie werden hierbei von der Leitung der jeweiligen Einrichtung unterstützt. IT-Sicherheitsbeauftragte sollten nicht Leiter bzw. Leiterinnen einer Einrichtung der HU sein.

(8) **IT-Systemverantwortliche, IT-Systemadministratoren**

Zu jedem IT-System muss eine IT-Systemverantwortliche oder ein IT-Systemveranwortlicher benannt sein. Zu den Aufgaben gehören:

- Planung, Einrichtung und Administration von IT-Systemen

[4] Der Verantwortungsbereich des genannten IT-Personals kann in Abstimmung mit den Leiterinnen und Leitern einrichtungsübergreifend sein, eine Person kann verschiedene der genannten Funktionen wahrnehmen.

- Gewährleistung des stabilen und sicheren Betriebes der IT-Systeme
- Organisation der Servicearbeiten für die Hard- und Software
- Erstellung eines Sicherheitskonzeptes für das jeweilige IT-System, Abstimmung mit der oder dem zuständigen IT-Sicherheitsbeauftragten
- Einhaltung der in dieser Richtlinie genannten Sicherheitsmaßnahmen
- zeitnahe Information der bzw. des zuständigen IT-Sicherheitsbeauftragen zu Problemen und Vorfällen hinsichtlich der IT-Sicherheit ihres Verantwortungsbereichs
- je nach Art der zu schützenden Daten die Veranlassung entsprechender Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit im jeweiligen Netz
- Information zu den Systemen und ihren Diensten sowie Dokumentation
- Einweisung und Beratung von Benutzerinnen und Benutzern

IT-Systemadministratoren sind für den technischen Betrieb von IT-Systemen zuständig. IT-Systemverantwortliche haben die technische Gesamtverantwortung für ein IT-System und sind in der Regel gleichzeitig IT-Systemadministrator. Systemverantwortliche und Systemadministratoren haben besondere Rechte hinsichtlich der Administration und des Datenzugriffs. Daraus resultiert eine hohe Verantwortung bezüglich des Datenschutzes und der Datensicherheit der IT-Systeme und ihrer Vernetzung.

(9) **IT-Personal der HU**

Zum IT-Personal der HU gehören IT-Systemverantwortliche und -administratoren, DV-Beauftragte, IT-Sicherheitsbeauftragte, Verantwortliche für IT-Verfahren und -Anwendungen.

(10) **IT-Benutzerinnen und -Benutzer**

Zu den IT- Benutzerinnen und Benutzern (IT-Anwender) gehören alle Personen, die IT-Systeme der HU benutzen. Sie sind zur Einhaltung aller in dieser Richtlinie genannten Maßnahmen verpflichtet.

(11) **Behördliche(r) Datenschutzbeauftragte(r)**

Die HU bestellt eine Mitarbeiterin oder einen Mitarbeiter zur Wahrnehmung der Aufgaben der oder des Behördlichen Datenschutzbeauftragten. Bestellung und Aufgaben sind im Berliner Datenschutzgesetz, BlnDSG § 19 a „Behördlicher Datenschutzbeauftragter“ beschrieben.

(12) **Personalvertretungen**

Die Funktion der Personalvertretungen ist im Personalvertretungsgesetz (PersVG) geregelt.

3. Maßnahmen zur Gewährleistung der IT-Sicherheit an der HU

Das übergreifende IT-Sicherheitskonzept der HU orientiert sich an der Methodik des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Gewährleistung eines IT-Grundschutzes [2].

In Anlagen dieser IT-Richtlinie sind universitätsweit geltende Maßnahmen des IT-Grundschutzes für IT-Anwender (s. Anlage 1) und für IT-Personal (s. Anlage 2) in Maßnahmenkatalogen zusammengestellt. Verantwortlichkeiten der Universitätsleitung, der Leiterinnen und Leiter von Einrichtungen, des IT-Personals und der Benutzerinnen und

Benutzer für die Initiierung und Durchführung von Maßnahmen zur Gewährleistung der IT-Sicherheit werden festgelegt. Diese Maßnahmen gehen von der an der HU vorhandenen und für Hochschulen typischen IT-Infrastruktur aus. Sie sind eine unbedingte Voraussetzung zur Gewährleistung des IT-Grundschutzes hinsichtlich der Aspekte Vertraulichkeit, Integrität und Verfügbarkeit bezogen auf IT-Systeme mit normalem Schutzbedarf entsprechend den Vorgaben des BSI. Maßnahmen für IT-Anwender gelten auch für IT-Personal.

Für jedes IT-System ist ein IT-Sicherheitskonzept erforderlich. In diesem sind Aspekte der Informationssicherheit zu analysieren und Sicherheitsmaßnahmen zu beschreiben. Für jedes IT-System ist durch eine Schutzbedarfsanalyse zu prüfen, ob ein über den Grundschutz hinausgehender Schutzbedarf vorliegt. Wird ein hoher oder sehr hoher Schutzbedarf nach BSI festgestellt, so sind geeignete zusätzliche Maßnahmen auf Grundlage einer Risikoanalyse im IT-Sicherheitskonzept festzulegen [3].

4. Inkrafttreten

Diese Richtlinie wird vom Präsidium der HU verabschiedet. Sie tritt am Tag nach ihrer Bekanntmachung im Amtlichen Mitteilungsblatt der HU in Kraft.

Anlage 1 Maßnahmen des IT-Grundschutzes für IT-Anwender

Allgemeines

M 1.1 Anwenderqualifizierung

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: IT-Systemverantwortliche, IT-Sicherheitsbeauftragte[5]

IT-Anwender sind nach Erfordernis aufgabenspezifisch einzuweisen und dürfen erst dann die IT-Infrastruktur nutzen. Dabei sind sie insbesondere auch mit den für sie geltenden Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes vertraut zu machen.

Die Schulung hat prinzipiell auch das allgemeine Sicherheitsbewusstsein und die Einsicht in die Notwendigkeit von IT-Sicherheitsmaßnahmen zu entwickeln.

Die Schulung sollte auch eine realistische Selbsteinschätzung fördern. Die IT-Anwender sollten erkennen, wann Experten hinzugezogen werden sollten.

An Stelle einer Schulung kann auch die Forderung nach selbständiger Einarbeitung stehen, wenn geeignete Beschreibungen zur Verfügung stehen.

M 1.2 Einhaltung einschlägiger Regelungen und Ordnungen

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

Die IT-Anwender sollten die einschlägigen internen Regelungen und Ordnungen für die Benutzung der Informationstechnik kennen, insbesondere die IT-Richtlinie der HU und die Benutzungsordnungen der IT-Betreiber (insbesondere Benutzungsordnung des CMS und der Universitätsbibliothek) und haben diese einzuhalten.

M 1.3 Einhaltung von Grundsätzen zur Benutzung der IT-Infrastruktur

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

Die IT-Infrastruktur der HU ist grundsätzlich zur Benutzung in Forschung, Lehre, Studium und Verwaltung vorgesehen.

Die Ressourcen der IT-Infrastruktur der HU sind effektiv und sparsam zu verwenden.

Jeder Missbrauch der IT-Infrastruktur der HU ist durch die IT-Anwender zu unterlassen. Dazu gehören unter anderem die unberechtigte Benutzung von IT-Ressourcen, das Eindringen in IT-Systeme bzw. der Versuch dazu, das Scannen der Netze bzw. der IT-Systeme zum Zweck der Informationsgewinnung über die Infrastruktur oder der unberechtigte Abgriff von Informationen im Netz oder auf IT-Systemen.

Jede Benutzung der IT-Infrastruktur, die zu Schäden an Technik, Programmen oder Daten führen kann bzw. die Personen schädigt oder belästigt, ist untersagt. Dazu gehört z. B. die Versendung von Schadprogrammen oder Spam-E-Mails.

Jede Benutzung der IT-Infrastruktur, die der Reputation der HU in Wissenschaft und Öffentlichkeit schaden kann, ist zu unterlassen.

Jeder Missbrauch von IT-Systemen der HU und jeder erkannte oder vermutete sicherheitsrelevante Vorfall ist unverzüglich dem zuständigen IT-Betreiber zu melden.

[5] Im Plural sind immer IT-Sicherheitsbeauftragte der Einrichtungen gemeint.

M 1.4 Einhaltung von Lizenzbestimmungen

Verantwortlich für Initiierung: DV-Beauftragte
Verantwortlich für Umsetzung: IT-Anwender

Bei der Benutzung von Software und Internet-basierten Diensten sind die jeweiligen Lizenzbestimmungen einzuhalten. Die IT-Anwender sind verpflichtet, sich über die Lizenzbestimmungen zu informieren.

M 1.5 Umgang mit personenbezogenen Daten

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: IT-Anwender

Die Erhebung, Verarbeitung und Speicherung personenbezogener Daten ist in BerDSG geregelt und grundsätzlich zu beachten. Ggf. ist die oder der behördliche Datenschutzbeauftragte der HU einzubeziehen.

M 1.6 Unterlassung strafbewehrter Handlungen

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

Es ist untersagt, insbesondere die nachfolgend benannten strafbewehrten Handlungen bei der Benutzung von IT-Systemen vorzunehmen:

- Ausspähen von Daten (§ 202 a StGB);
- Verletzung des Datenschutzes (§ 32 BlnDSG, § 43 - 44 BDSG);
- Datenveränderung (§ 303 a StGB) und Computersabotage (§ 303 b StGB);
- Computerbetrug (§ 263 a StGB);
- Verbreitung pornographischer Darstellungen (§ 184 StGB), insbesondere Abruf oder Besitz kinderpornographischer Darstellungen (§ 184 Abs. 5 StGB);
- Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB);
- Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB);
- Strafbare Urheberrechtsverletzungen, z. B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG).

M 1.7 Meldung von Sicherheitsproblemen

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

Auftretende Sicherheitsprobleme aller Art (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u.a.) sind dem zuständigen IT-Betreiber mitzuteilen.
Jeder schwerwiegende Vorfall ist zu dokumentieren und der oder dem IT-Sicherheitsbeauftragten und der Leiterin oder dem Leiter der Einrichtung zu melden.

M 1.8 Ahndung persönlicher Sicherheitsverstöße

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Leiter/in der Personal- bzw. Studienabteilung

Als zu ahndender Sicherheitsverstoß gilt die vorsätzliche oder grob fahrlässige Nichtbeachtung der IT-Richtlinie der HU, insbesondere wenn sie

- die Sicherheit von Personen oder des Vermögens der HU in erheblichen Umfang beeinträchtigt,
- der HU erheblichen finanziellen Verlust durch Kompromittieren der Sicherheit von Daten oder Geschäftsinformationen einbringt,

- den unberechtigten Zugriff auf Systeme und Informationen, deren Preisgabe und/oder Änderung beinhaltet,
- die Nutzung von Informationen der HU für illegale Zwecke beinhaltet und
- den unbefugten Zugriff auf personenbezogene Daten ermöglicht.

Sicherung der Infrastruktur

M 1.9 Räumlicher Zugangsschutz

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: IT-Anwender

Der unbefugte Zugang zu IT-Geräten und die unbefugte Nutzung müssen verhindert werden. Bei Abwesenheit sind Räume mit Informationstechnik 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.

M 1.10 Brandschutz

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: IT-Anwender

Alle Maßnahmen und Einrichtungen, die dem vorbeugenden Brandschutz dienen, sind einzuhalten bzw. zu nutzen. Lüftungsöffnungen an den Geräten dürfen nicht verstellt oder verdeckt werden. In allen Räumen, in denen Server und Netzwerkkomponenten untergebracht sind, sind alle Tätigkeiten zu unterlassen, die zu einer Rauchentwicklung führen. Fluchtwege sind frei zu halten.

M 1.11 Sicherung mobiler Computer

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

Bei der Speicherung von schützenswerten Daten auf mobilen Computern sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Insbesondere ist eine hinreichend sichere Verschlüsselung anzuwenden.

Mobile Computer sind nicht unbeaufsichtigt zu lassen bzw. sind verschlossen und nach außen nicht sichtbar aufzubewahren (z. B. im Kfz).

Auf Datensicherung mobiler Computer ist besonders Wert zu legen.

Hard- und Software

M 1.12 Kontrollierter Softwareeinsatz

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

Auf Computersystemen der HU darf zum Zweck des Schutzes der IT-Infrastruktur nur Software installiert und genutzt werden, die vertrauenswürdig und zur Erfüllung der dienstlichen Aufgaben erforderlich ist. Besondere Vorsicht ist bei Software, die aus dem Internet heruntergeladen wurde, oder bei Software aus E-Mail-Anhängen geboten, damit weder das IT-System noch das Universitätsnetz gefährdet bzw. beeinträchtigt werden. Im Zweifelsfall ist die Zustimmung der/des IT-Sicherheitsbeauftragten der Einrichtung einzuholen.

M 1.13 Einsatz von privater oder nicht von IT-Personal betriebener Hard- und Software

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

Die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der HU und deren Netzen ist in der Regel nicht gestattet. Das gilt insbesondere in speziell abgesicherten Netzbereichen (z. B. Verwaltungsnetz der HU). Die Leitung der betreffenden Einrichtung kann Ausnahmen gestatten, wenn der Einsatz zur Erfüllung dienstlicher Aufgaben erforderlich ist und Sicherheitsbelange dem nicht entgegen stehen.
Allgemeine Ausnahmen gelten für den Einsatz von privaten Computern für Lehrveranstaltungen und Vorträge, in speziell gekennzeichneten Bereichen (zum Beispiel in Bibliotheken oder in Studierendenarbeitsbereichen), im WLAN der HU sowie bei der Nutzung des Netzes der HU über VPN.
Die im Netz der HU verwendete private Hard- und Software muss die IT-Sicherheits-anforderungen dieser IT-Richtlinie berücksichtigen.
Der Einsatz von Hard- und Software, die der HU gehört, die aber nicht IT-Personal der HU administriert wird, unterliegt vergleichbaren Einschränkungen wie der Einsatz privater Hard- und Software. Voraussetzung für den Einsatz dieser Hard- und Software ist eine Zustimmung durch den zuständigen IT-Sicherheitsbeauftragten.

M 1.14 Schutz vor Schadprogrammen, Absicherung der Computer

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

Das Eindringen von Schadsoftware auf Arbeitsplatzcomputer muss verhindert werden. Neben der Gefährdung bzw. Schädigung des betroffenen Computers gehen von Schadsoftware Gefahren für andere IT-Systeme im HU-Netz (Folge: Beeinträchtigung der Arbeitsfähigkeit der HU) und ggf. darüber hinaus für Systeme außerhalb des HU-Netzes (Folgen: Regressanforderungen an die HU, Beeinträchtigung der Reputation der HU) aus.
Auf allen Arbeitsplatzcomputern ist ein aktueller Scanner für Schadprogramme einzurichten, der automatisch alle eingehenden Daten und alle zu öffnenden Dateien überprüft. Es ist vorzugsweise die vom CMS zur Verfügung gestellte Antiviren-Software zu verwenden. Regelmäßig und automatisiert sind die Virenerkennungsmuster zu aktualisieren. Wird auf einem System schädlicher Programmcode entdeckt, muss dies dem zuständigen IT-Sicherheitsbeauftragten gemeldet und das Ergebnis der eingeleiteten Maßnahmen dokumentiert werden.

In regelmäßigen Abständen sowie bei konkretem Bedarf oder Verdacht ist mit dem Scan-Programm eine Suche nach Schadprogrammen vorzunehmen.

Von Herstellern bereitgestellte Softwareaktualisierungen zur Beseitigung von Sicherheitslücken sind einzuspielen.

Im Betriebssystem enthaltene Firewall-Funktionen oder eine vorhandene gleichwertige Firewall-Funktionalität durch Programme anderer Hersteller sind zu aktivieren.

Anwendungen – insbesondere Netzanwendungen wie Mailprogramme und Web-Browser – sind sicher zu konfigurieren, so dass Schadprogramme nicht unnötig leicht aktiv werden können.

Erweiterte Rechte (Administrator, root) sind nur in Anspruch zu nehmen, wenn das für einen Arbeitsvorgang unabdingbar ist.

Zugriffsschutz

M 1.15 Abmelden und ausschalten

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

Beim Verlassen ungesicherter Arbeitsräume soll der Arbeitsplatzcomputer durch einen Kennwortschutz gesperrt werden. Bei längerer Abwesenheit sollte sich die Benutzerin bzw. der Benutzer aus den laufenden Anwendungen und dem Betriebssystem abmelden. Grundsätzlich müssen die Systeme nach Dienstschluss gesichert oder ausgeschaltet sein. Von diesen Regelungen kann nur abgewichen werden, soweit es die Arbeitsorganisation dringend erfordert und/oder andere Sicherheitsmaßnahmen es ermöglichen.

M 1.16 Personenbezogene Kennungen (Authentifizierung)

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

Alle Computersysteme sind so einzurichten, dass nur berechtigte Personen die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine Anmeldung mit Benutzerkennung und Passwort oder per zertifikatsbasierter Chipkarte 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 grundsätzlich unzulässig. Es ist untersagt, Passwörter und Chipkarten weiterzugeben.

Ausgenommen von dieser Regelung sind Systeme, die für allgemeine öffentliche Zugänge mit eingeschränkter Nutzung des HU-Netzes bestimmt sind (z. B. Kiosksysteme, Abfragestationen für Bibliothekskataloge).

M 1.17 Gebrauch von Passwörtern, Chipkarten, PINs und privaten Schlüsseln

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Systemverantwortliche, IT-Anwender

Persönliche Passwörter, PINs und z. B. zur Verschlüsselung verwendete private Schlüssel müssen geheim gehalten werden und sollten nur der berechtigten Person persönlich bekannt sein. Sofern eine Aufbewahrung von Passwort bzw. PIN erforderlich ist, muss diese so erfolgen, dass sie nur durch den Benutzer einsehbar sind (verschlossen bzw. verschlüsselt).

Persönliche Passwörter, PINs, private Schlüssel und Chipkarten dürfen nicht weitergegeben werden.

Für die Wahl und Handhabung von Passwörtern bzw. PINs sind folgende Regeln zu beachten:

- Ein Passwort muss hinreichend lang sein. Passworte und PINs dürfen nicht leicht zu erraten sein. Voreingestellte Passwörter und PINs müssen durch individuelle ersetzt werden. Vorgaben der Betreiber hinsichtlich Auswahl und Wechsel von Passworten und PINs sind zu beachten.
- Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.
- Die Eingabe von Passwort bzw. PIN muss unbeobachtet stattfinden.
- Wenn Passwort bzw. PIN nichtautorisierten Personen bekannt geworden sind, ist ein Passwort- bzw. PIN-Wechsel durchzuführen.

M 1.18 Zugriffsrechte (Autorisierung)

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

Benutzerinnen und Benutzer sollten nur mit den Zugriffsrechten ausgestattet werden, die für die Erledigung ihrer Aufgaben vorgesehen sind.

M 1.19 Netzzugänge

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

Der Anschluss von Systemen an das Datennetz der HU hat ausschließlich über die dafür vom Netzbetreiber (CMS) vorgesehene Infrastruktur zu erfolgen.

Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Datenleitungen, Switche, Modems, WLAN-Accesspoints o. ä.) ist unzulässig. Ausnahmen darf nur der Netzbetreiber in Absprache mit der bzw. dem zuständigen IT-Sicherheitsbeauftragten einrichten bzw. beauftragen.

An das Datennetz dürfen nur die dafür vorgesehenen IT-Systeme an den durch den Netzbetreiber (CMS) vorgesehenen Stellen angeschlossen werden.

Kommunikationssicherheit

M 1.20 Sichere Netzwerknutzung

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

Der Einsatz von verschlüsselten Kommunikationsdiensten ist, sofern technisch möglich, den unverschlüsselten Diensten vorzuziehen. Die Übertragung schützenswerter Daten muss verschlüsselt erfolgen (z. B. vertrauliche E-Mails, Personendaten, Passwörter). Bei externen Zugriffen auf interne Netzdienste der HU sind VPN-Techniken einzusetzen.

Datensicherung

M 1.21 Datensicherung

Verantwortlich für Initiierung: IT-Systemverantwortliche für Datensicherung
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen o. ä. schützen. Grundsätzlich sind Daten von Arbeitsplatzcomputern auf zentralen Servern zu speichern. Ist die Speicherung auf zentralen Servern nicht möglich, sind die Benutzerinnen und Benutzer für die Sicherung ihrer Daten selbst verantwortlich.

Bei zentraler Datensicherung müssen sich die Benutzerinnen und Benutzer über die beim jeweiligen Betreiber geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung informieren.

Umgang mit Datenträgern und schützenswerten Daten

M 1.22 Umgang mit Datenträgern

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

Mobile Datenträger mit schützenswerten Daten sind verschlossen und vor unbefugtem Zugriff geschützt aufzubewahren. Die Lagerbedingungen gemäß den Herstellerangaben sind

einzuhalten. Insbesondere ist darauf zu achten, dass ein hinreichender Schutz gegen Staub, Hitze, Licht, Feuchtigkeit und magnetische Felder besteht.

Datenträger sind zu kennzeichnen falls die Identifikation des Datenträgers nicht durch ein anderes technisches Verfahren erfolgt. Ausnahmen können z. B. Datenträger bilden, die ausschließlich der persönlichen Nutzung vorbehalten sind (z. B. persönliche USB-Sticks).

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.

Datenträger müssen beim Transport vor Beschädigungen geschützt sein.

Die Übermittlung von Datenträgern mit vertraulichen Daten hat dem Schutzbedarf angemessen zu erfolgen (Verschlüsselung, Versandart, Verpackung, Kontrolle des Empfangs, Protokollierung).

M 1.23 Physisches Löschen von Datenträgern

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

Datenträger mit schützenswerten Daten müssen vor einer Weitergabe an nicht autorisierte Personen physisch gelöscht werden.

Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), mit speziellen Verfahren vollständig unlesbar gemacht bzw. mechanisch zerstört werden. Im Zweifelsfall sind Daten auf dem Datenträger als schützenswert zu betrachten.

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

Weitere Informationen und Auskünfte zum Löschen von Datenträgern geben die Benutzerberatung des CMS und die bzw. der Datenschutzbeauftragte der Universität.

M 1.24 Schützenswerte Daten auf Arbeitsplatzcomputern

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

Prinzipiell sind die Benutzerinnen und Benutzer dafür verantwortlich, den Schutzbedarf ihrer Daten einzuschätzen und geeignete Maßnahmen einzuleiten. Beim Speichern schützenswerter Daten auf Festplatten von Arbeitsplatzcomputern oder anderen lokalen Speicher- oder Übertragungsmedien und bei deren Übertragung ist auf Verschlüsselung zu orientieren, sofern nicht anderweitige Schutzmaßnahmen einen hinreichenden Schutz bieten.

Anlage 2 Maßnahmen des IT-Grundschutzes für IT-Personal

Die im Folgenden beschriebenen Maßnahmen richten sich an das Leitungs- und das IT-Personal der HU. Die in der Anlage 1 der IT-Richtlinie der HU beschriebenen Maßnahmen für IT-Anwender sind auch für IT-Personal verbindlich.

Allgemeines

M 2.1 Verantwortung für IT-Einsatz und IT-Sicherheit

Verantwortlich für Initiierung: LGI
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen, IT-Personal

Die Verantwortung für die Umsetzung und Einhaltung der für den IT-Einsatz geltenden Regelungen, dabei insbesondere der Regelungen zur Gewährleistung der IT-Sicherheit, tragen die Leiterinnen bzw. Leiter der Einrichtungen und das IT-Personal entsprechend der IT-Richtlinie der HU.

M 2.2 Bekanntmachung von Richtlinien und Zuständigkeitsregelungen

Verantwortlich für Initiierung: LGI
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen

Die IT-Richtlinie der HU ist dem IT-Personal der HU bekannt zu machen. Die Kenntnisnahme ist zu dokumentieren.

Über zusätzliche Richtlinien und Zuständigkeitsregelungen für einzelne Bereiche oder spezielle Verfahren sind alle betroffenen Mitarbeiterinnen und Mitarbeiter entsprechend zu informieren.

Über alle Änderungen an Richtlinien und Zuständigkeitsregelungen ist umgehend zu informieren.

M 2.3 IT-Sicherheitsbeauftragte der Einrichtungen

Verantwortlich für Initiierung: LGI
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen

Den IT-Sicherheitsbeauftragten der Einrichtungen kommt im Rahmen des IT-Sicherheitskonzeptes der HU eine besondere 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 und führen die notwendigen Aufzeichnungen in ihrem Verantwortungsbereich. Bei Fragen des sicheren IT-Einsatzes sind sie Ansprechpartner sowohl für die Mitarbeiterinnen und Mitarbeiter ihrer Einrichtung als auch für Dritte (z. B. CMS).

Die Leiterinnen bzw. Leiter der Einrichtungen sind dafür verantwortlich, dass alle IT-Systeme ihrer Einrichtung dem Zuständigkeitsbereich einer bzw. eines IT-Sicherheitsbeauftragten zugeordnet sind.

Organisation von IT-Sicherheit

M 2.4 Frühzeitige Berücksichtigung von IT-Sicherheitsfragen

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte, IT-Personal

Fragen der IT-Sicherheit sind bei Neubeschaffungen von IT-Systemen und der Einführung neuer IT-Verfahren schon im Planungsstadium zu berücksichtigen.

M 2.5 Rollentrennung

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Personal

Für jedes IT-System sind die Verantwortlichkeiten für alle Bereiche eindeutig festzulegen und zu dokumentieren.
Normalerweise ist eine Rollentrennung von Verfahrensentwicklung/-pflege und Systemadministration sinnvoll. Jeder Mitarbeiterin und jedem Mitarbeiter müssen die ihr bzw. ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein. Abgrenzungen und Schnittflächen der verschiedenen Anwenderrollen müssen klar definiert sein.

M 2.6 Dokumentation und Sicherheitskonzept der IT-Verfahren, -Dienste und -Systeme

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Verantwortliche für IT-Verfahren, -Dienste und -Systeme

IT-Verfahren, -Dienste und -Systeme müssen aktuell dokumentiert werden. Die Dokumentation muss den Betrieb auch bei personellen Vertretungen absichern. Es muss ein Sicherheitskonzept vorliegen. Informationen zur Benutzung der Dienste sind zur Verfügung zu stellen.

Zum Sicherheitskonzept eines IT-Systems gehören u. a. folgende Angaben:

- Aufgaben/Ziele des Verfahrens/Dienstes/Systems
- Verantwortungsbereiche, personelle Absicherung
- Kurzbeschreibung des Verfahrens/Systems (Übersicht, Hardware, Software, Infrastruktur)
- Schnittstellen zu anderen Verfahren/Systemen
- Datenbeschreibung, Aussagen zum Schutzbedarf, Umgang mit Protokolldaten
- Risikoanalyse bei erhöhtem Schutzbedarf
- Maßnahmen zur Gefahrenabwendung (sichere Infrastruktur, Technikredundanz, Netz- und Serversicherheit, Rollendefinition und Zugriffsrechte, Datensicherung, personelle Absicherung und Verpflichtung)
- Notfallvorsorge (Wartungsstrategie, Systemüberwachung, Sicherungsstrategie)

IT-Sicherheitsbeauftragte initiieren und kontrollieren die Sicherheitskonzepte der IT-Verfahren, -Dienste und -Systeme ihrer Verantwortungsbereiche.

Sofern personenbezogene Daten verarbeitet bzw. gespeichert werden, ist grundsätzlich § 19 Abs. 2 BlnDSG einzuhalten. Insbesondere ist eine entsprechende Dateibeschreibung erforderlich. Die oder der behördliche Datenschutzbeauftragte der HU ist einzubeziehen.

Bei Auswirkungen der IT-Systeme auf das Personal der HU, insbesondere wenn Möglichkeiten für Rückschlüsse auf das Verhalten des Personals bestehen, ist der zuständige Personalrat einzubeziehen.

M 2.7 Information zu Störungen der IT-Systeme und der Systemverfügbarkeit

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: IT-Personal

Über Störungen der Dienste ist durch die IT-Betreiber in geeigneter Weise zu informieren.

M 2.8 Dokumentation von sicherheitsrelevanten Ereignissen und Fehlern

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Personal

Sicherheitsprobleme und Ereignisse, die Indiz für ein Sicherheitsproblem sein können, sind der bzw. dem zuständigen IT-Sicherheitsbeauftragten und dem Betreiber des Systems zu

melden. Sie sind von diesen zu dokumentieren. Das trifft insbesondere auch auf Sicherheitsprobleme und -vorfälle zu, die für die übergreifende IT-Sicherheit von Bedeutung sein können. Die IT-Sicherheitsbeauftragten melden relevante Vorfälle regelmäßig oder bei Bedarf sofort der bzw. dem IT-Sicherheitsbeauftragten der HU.

Bei sicherheitsrelevanten Vorfällen, die möglicherweise Straftatbestände berühren, wird die Einbeziehung der Rechtsstelle der HU empfohlen.

M 2.9 Regelungen der Auftragsdatenverarbeitung

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Verantwortliche für IT-Verfahren und IT-Systeme

Eine schriftliche Vereinbarung ist für alle im Auftrag der HU betriebenen IT-Verfahren und -Systeme Voraussetzung. Es sind eindeutige Zuweisungen der Verantwortlichkeiten 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 (BlnDSG) bzw. des Bundesdatenschutzgesetzes (BDSG) zu beachten.

Der oder die behördliche Datenschutzbeauftragte der HU ist schon im Vorfeld der Auftragsdatenverarbeitung personenbezogener Daten einzubeziehen.

M 2.10 Standards für die technische Ausstattung

Verantwortlich für Initiierung: LGI
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragte(r) der HU, IT-Betreiber

Zur Erreichung eines ausreichenden Sicherheitsniveaus für IT-Systeme sind Qualitätsstandards im Sinne der IT-Richtlinie der HU von der bzw. dem IT-Sicherheitsbeauftragten der HU in Zusammenarbeit mit dem CMS und dezentralen IT-Betreibern unter Maßgabe der durch die LGI definierten Strategien festzulegen.

M 2.11 Revision der IT-Sicherheit

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Systemverantwortliche

Alle eingesetzten IT-Sicherheitsmaßnahmen müssen auf ihre Tauglichkeit, Wirksamkeit und Einhaltung überprüft werden. Diese Überprüfung muss regelmäßig (auch unangekündigt) und nach jeder relevanten Änderung der Sicherheitsstandards erfolgen. Dies kann mit Hilfe entsprechender Tools oder durch externe Dienstleister durchgeführt werden. Primäres Ziel der Kontrollen ist es Mängel festzustellen, ihre Ursachen zu ermitteln und Lösungen aufzuzeigen, beispielsweise durch die Änderung bestehender Regelungen oder durch neue technischer Maßnahmen.

Maßnahmen welche die Sicherheit von IT-Systemen in einem Netzbereich testen (z. B. Portscans), sind mit dem Netzbetreiber (CMS) abzustimmen.

Personelle Maßnahmen

M 2.12 Sorgfältige Personalauswahl

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen

Mit Administrationsaufgaben auf Netzwerk- und Systemebene sollten nur sorgfältig ausgewählte, ausreichend qualifizierte, vertrauenswürdige, zuverlässige und motivierte Mitarbeiterinnen und Mitarbeiter betraut werden. Kurzzeitig befristet Beschäftigte (Beschäftigungsverhältnis von weniger als einem Jahr) sollten nach Möglichkeit keine Aufgaben übernehmen, die nur mit Administratorrechten ausgeführt werden können. Das

eingesetzte Personal ist darauf hinzuweisen, dass seine Befugnisse nur für die erforderlichen Administrationsaufgaben verwendet werden dürfen und dass eine besondere Verantwortung hinsichtlich des Datenschutzes und der Datensicherheit besteht.

M 2.13 Vertretung

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen, IT-Systemverantwortliche

Für Systembetreuungs- und -administrationsfunktionen sind Vertretungsregelungen erforderlich. Die Vertreterinnen bzw. Vertreter müssen alle notwendigen Tätigkeiten ausreichend beherrschen und auf schriftliche Arbeitsanweisungen und Dokumentationen zurückgreifen können. Die Vertretungsregelung sollte im System abgebildet sein und nicht durch die Weitergabe von Passwörtern erfolgen.

Vertretungsrechte sollten im System möglichst ständig eingerichtet sein. Eine Ausnahme bilden systemspezifische, nicht nutzerabhängige Kennungen (zum Beispiel root bei UNIX-Systemen). Hier soll nach Möglichkeit nur im Bedarfsfall auf das an geeigneter Stelle hinterlegte Administrator-Passwort zurückgegriffen werden können.

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

M 2.14 Qualifizierung

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte

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.

Sicherung der Infrastruktur

M 2.15 Sicherung der Server- und Speicherräume

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Technische Abteilung

IT-Systeme mit typischer Serverfunktion sowie Speichersysteme 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 eines gewaltsamen Eindringens vorzusehen. Die Türen müssen mit chipkartenbasierten Schließsystemen versehen sein und sollen selbsttätig schließen; verwendete Chipkarten und Schlüssel müssen kopiergeschützt sein.

Für die Chipkarten- und Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen. Der Zutritt muss auf diejenigen Personen begrenzt werden, deren Arbeitsaufgaben dieses erfordert.

In einem Server-/Speicherraum sollten sich keine Geräte oder Ausrüstung befinden, die den Zutritt für einen erweiterten Benutzerkreis erforderlich machen (z. B. Kopierer).

M 2.16 Geschützte Aufstellung von IT-Systemen

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Systemverantwortliche

IT-Systeme sind in gesicherten Räumen aufzustellen. 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.
- Eine direkte Lichteinstrahlung auf Bildschirme ist aus ergonomischen Gründen zu vermeiden.

M 2.17 Sicherung der Netzknoten

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Technische Abteilung

Vernetzungsinfrastruktur (Switches, Router, Verteilertechnik 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 2.15 - Sicherung der Server- und Speicherräume. Chipkartenbasierte Schließsysteme sind je nach Schutzbedürftigkeit, mindestens aber für die zentralen Verteilerräume der Gebäude vorzusehen.

M 2.18 Verkabelung, Netztechnik, Funknetze

Verantwortlich für Initiierung: Technische Abteilung, Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Technische Abteilung, IT-Betreiber

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.

Die Verkabelung und die Netztechnik des LANs sind klar zu strukturieren sowie aktuell und vollständig zu dokumentieren, z. B. durch geeignete Netzwerk- und Kabelmanagementsysteme. Die IT-Systemverantwortlichen müssen für ihre Verantwortungsbereichen einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung der Netzwerkkomponenten haben.

Erweiterungen und Veränderungen an der Gebäudeverkabelung und an Geräten des Netzes, einschließlich der Funknetze, sind nur durch die Betreiber gestattet (Technische Abteilung, CMS).

Die zwischen der Technischen Abteilung und dem CMS abgestimmten „Parameter der HU-Gebäudeverkabelung“ und das „Bezeichnungsschema für Kabel, Verteilerports und Anschlussdosen“ sind einzuhalten.

Der Anschluss von Geräten an das Netz ist in Abstimmung mit dem CMS in der Regel durch eingewiesene lokale Verantwortliche durchzuführen.

M 2.19 Einweisung und Beaufsichtigung von Fremdpersonal, Fremdwartung

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte

Der Zutritt nicht autorisierter Personen (z. B. Wartungs- oder Reinigungspersonal der HU oder von Firmen) zu IT-Räumen darf nur mit Genehmigung eines für den Raum Verantwortlichen erfolgen. Sie sind nach Möglichkeit zu beaufsichtigen. Der Zutritt ist zu dokumentieren.

Personen, die nicht unmittelbar zum IT-Bereich zu zählen sind, aber Zugang zu gesicherten IT-Räumen benötigen, müssen über das Verhalten in IT-Räumen belehrt werden.

Für Wartungsarbeiten stellen die Datenschutzgesetze besondere Regelungen bereit, die anzuwenden sind. Wenn bei Arbeiten durch externe Firmen vor Ort oder per Fernwartung, die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, müssen die ausführenden Personen gemäß BlnDSG verpflichtet sein. Das betrifft insbesondere auch das Datengeheimnis.

Für die Wartung und Instandhaltung sind Verträge gemäß § 3, 3a BlnDSG bzw. § 11 BDSG zu schließen. Das Prinzip der Zweckbindung nach § 11 BlnDSG bzw. § 31 BDSG ist zu beachten.

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

M 2.20 Gesicherte Stromversorgung und Überspannungsschutz

Verantwortlich für Initiierung: Technische Abteilung, Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Technische Abteilung, IT-Personal

Alle wichtigen IT-Systeme dürfen nur an eine ausreichend dimensionierte und gegen Überspannungen abgesicherte Stromversorgung angeschlossen werden. Eine entsprechende Versorgung ist durch die Technische Abteilung herzustellen. Überspannungsschutzeinrichtungen sollten periodisch und nach bekannten Ereignissen geprüft und ggf. ersetzt werden.

Bei Einsatz von Geräten mit redundant ausgelegter Stromversorgung ist darauf zu achten, dass die einzelnen Netzteile über getrennt abgesicherte Stromkreise versorgt werden.

M 2.21 Unterbrechungsfreie Stromversorgung (USV), Notstromversorgung

Verantwortlich für Initiierung: Technische Abteilung, Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Technische Abteilung, IT-Betreiber

Alle IT-Systeme, die wichtige oder unverzichtbare Beiträge zur Aufrechterhaltung eines geordneten Betriebes leisten, wie zum Beispiel Server, Speicher und zentrale Netzwerkkomponenten, sind an unterbrechungsfreie Stromversorgungen (USV) zur Überbrückung von Ausfällen und Schwankungen der Stromversorgung anzuschließen. Die USV-Systeme müssen Ausfälle signalisieren (über SNMP an die versorgten Systeme, bei zentralen USV auch an die Gebäudeleittechnik), ihre Dimensionierung und Konfiguration müssen eine für das kontrollierte Herunterfahren der versorgten IT-Systeme ausreichende Haltezeit gewährleisten.

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

Eine regelmäßige und protokollierte Wartung der USVs ist sicherzustellen.

IT-Raumkomplexe des CMS von herausgehobener Bedeutung für die Arbeitsfähigkeit der gesamten HU sind nach Möglichkeit durch Notstromaggregate abzusichern.

M 2.22 Brandschutz

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, Brandschutzobmann, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Technische Abteilung, Leiter/innen der Einrichtungen

Einzuhalten sind die „Brandschutzgrundsätze für den Hochschulbereich der Humboldt-Universität zu Berlin“ sowie die Brandschutzordnungen der Einrichtungen der HU.

Die Regeln des vorbeugenden Brandschutzes sind besonders wichtig für Räume mit wichtiger Informationstechnik, wie beispielsweise Serverräume. Brandlasten sind zu minimieren. Papier, leere Verpackungen und andere leicht entflammbare Materialen dürfen in diesen Räumen nicht gelagert werden. Es besteht prinzipielles Rauchverbot.

M 2.23 Schutz vor Wasserschäden

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: Technische Abteilung

IT-Systeme, die wichtige oder unverzichtbare Komponenten zur Aufrechterhaltung eines geordneten Betriebes darstellen, sind nicht in direkter Nähe zu oder unter wasserführenden Leitungen aufzustellen. Auch bei einem Wassereinbruch muss der weitere Betrieb der IT-Systeme gewährleistet sein. Bei möglichen Gefährdungen sind Wasserschutz, Wassermelder, Abflüsse und Pumpen zu installieren und regelmäßig zu prüfen. Dies gilt insbesondere dann, wenn die IT-Systeme in Kellerräumen oder unterhalb von wasserführender Klimatisierungstechnik aufgestellt werden. So ist beispielsweise besonders darauf zu achten, dass nicht die tiefste Stelle im Gebäude zur Aufstellung der Geräte genutzt wird.

M 2.24 Klimatisierung

Verantwortlich für Initiierung: Technische Abteilung, Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Technische Abteilung, IT-Betreiber

Der Einbau von Klimatisierungsanlagen wird erforderlich, wenn der Luft- und Wärmeaustausch von Server-, Speicher- und Verteilerräumen 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. Überwachungssysteme mit Fehlersignalisierung sind vorzusehen. Klimatisierungsanlagen sind an geeigneter Stelle aufzustellen und regelmäßig zu warten. Die Stromversorgung der Klimatechnik ist entsprechend der Stromversorgung der zu klimatisierenden Technik abzusichern.

In klimatisierten Räumen, die ständig mit Personal besetzt sind, ist eine Frischluft-Beimischung notwendig.

Hard- und Softwareeinsatz

M 2.25 Planung, Beschaffung, Softwareentwicklung

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragte, IT-Systemverantwortliche

Die Planung und Beschaffung von sicherheitsrelevanter Soft- und Hardware ist mit den zuständigen IT-Sicherheitsbeauftragten abzustimmen. Dazu sind einzusetzende IT-Systeme und zu entwickelnde bzw. dann einzusetzende Software im Vorfeld der Beschaffung bzw. Entwicklung an diese zu melden.

Bei der Planung eines IT-Systems bzw. vor der Entwicklung von Software durch IT-Betreiber der HU ist eine Projektvorstellung in einem geeigneten und offenen Rahmen des IT-Betreibers erforderlich.

M 2.26 Kontrollierter Softwareeinsatz

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Personal

Auf Serversystemen der HU darf nur benötigte Software aus vertrauenswürdigen Quellen installiert werden (z. B. gekaufte Software, Open-Source-Software, selbst entwickelte Software). Von der Software darf keine Gefährdung für das IT-System bzw. das Netzwerk ausgehen. Im Zweifelsfall ist die Zustimmung der Leiterin bzw. des Leiters der betreffenden Einrichtung einzuholen.

In der Regel sollte auf Serversystemen keine typische Client-Software installiert sein. Ausgenommen davon sind Server, deren typische Aufgabe es ist, Anwendern Client-Software zur Verfügung zu stellen (z. B. Terminalserver).

M 2.27 Separate Entwicklungs- und Testumgebung, Schulungssysteme

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

Die Entwicklung oder Anpassung von serverbasierter Software sollte nicht in der Produktionsumgebung sondern muss in einer Testumgebung erfolgen. Der Testverlauf und dabei insbesondere Sicherheitsaspekte sind zu dokumentieren.

Eine Verarbeitung von personenbezogenen Realdaten in Entwicklungs- und Testumgebungen ist soweit möglich zu vermeiden. Ggf. ist der oder die behördliche Datenschutzbeauftragte einzubeziehen. Das gilt in gleicher Weise, wenn personenbezogene Realdaten in Schulungssystemen verwendet werden sollen.

M 2.28 Schutz vor Schadsoftware, Absicherung der Computer

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

Es gelten, soweit anwendbar, die Hinweise in Maßnahme M 1.14.

Das IT-Personal hat im eigenen Verantwortungsbereich dafür Sorge zu tragen, dass die unter M 1.14. beschriebenen Maßnahmen auf Servern und Client-Computern umgesetzt werden. Sollte durch Benutzerinnen oder Benutzer der Verdacht auf Schadsoftware gemeldet werden, sind durch einen Administrator die betroffenen Systeme zu ermitteln, die weitere Ausbreitung zu verhindern und die Systeme in einen betriebsbereiten Zustand zurückzuversetzen.

Nachdem alle Schadprogramme entfernt worden sind, müssen alle von diesem Computer aus genutzten Zugangskennungen und Passwörter geändert werden, um einem möglichen Missbrauch vorzubeugen.

Sollte ein Computer nicht mit Gewissheit von Schadsoftware befreibar sein, sollten Betriebssystem und Programme neu installiert werden. Bei Servern wird nach einem Befall mit Schadsoftware grundsätzlich eine Neuinstallation empfohlen.

In Serverbetriebssystemen enthaltene Sicherheitsfunktionalität oder eine gleichwertige Funktionalität durch Programme anderer Hersteller ist zu aktivieren.

Nicht benötige Serverfunktionen sind zu deaktivieren, so dass der Server nur auf den Ports (TCP/UDP) Verbindungen entgegen nimmt, die für die Funktion des Servers notwendig sind.

Die Serveradministration ist nur über gesicherte Verbindungen zulässig.

Systemverantwortliche für Mailserver müssen Maßnahmen zur Verhinderung der Zustellung von Schadprogrammen und zur Vermeidung von Spam-E-Mails vorsehen.

Bei der Installation umfangreicher Updates bzw. neuer Softwareversionen ist die notwendige Vorsicht walten zu lassen (ggf. Tests, Abwarten der nächsten Version), sofern es sich nicht um wichtige Sicherheitsupdates handelt.

Die Integrität und Authentizität der einzuspielenden Sicherheitsupdates und Patches ist sicherzustellen (Nutzung vertrauenswürdigen Quellen).

Auf Servern sollten nur Dienste mit vergleichbarem Schutzbedarf installiert sein. Die Netzeinbindung eines Servers muss den Schutzbedarf seiner Daten berücksichtigen. Es ist eine Bildung von Zonen mit jeweils vergleichbarem Schutzbedarf vorzusehen. Ggf. ist der Einsatz zusätzlicher Sicherheitstechnik (z. B. Firewall, Intrusion Prevention) erforderlich.

Das IT-Personal muss sich über veröffentlichte Schwachstellen der verwendeten Software aktiv informieren.

M 2.29 PCs mit erhöhtem Schutzbedarf

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: IT-Personal

Bei erhöhtem Schutzbedarf müssen alle äußeren Zugänge des PCs (zum Beispiel Disketten- und CD-ROM-Laufwerke, USB-Anschlüsse, Wechseldatenträger) gesperrt werden, wenn sie für die zu erledigenden Aufgaben nicht notwendig sind. Die Möglichkeit der Nutzung von Applikationsservern und laufwerkslosen Arbeitsplatzcomputern bzw. Terminals ist zu prüfen.

M 2.30 Ausfallsicherheit

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Betreiber, IT-Personal

Maßnahmen zur Ausfallsicherheit sind entsprechend der jeweiligen Anforderung zu ergreifen. IT-Systeme, die zur Aufrechterhaltung des Universitätsbetriebes grundlegend wichtig sind, müssen durch Ausweichlösungen (redundante Geräteauslegung oder Übernahme durch gleichartige Geräte) oder Wartungsverträge mit kurzen Reaktionszeiten hinreichend sowie durch eine redundante Infrastruktur (Stromversorgung, Klimatisierung) verfügbar gehalten werden.

Sind mehrere geeignete Aufstellmöglichkeiten für IT-Systeme vorhanden, sollten redundante Geräte nach Möglichkeit in verschiedenen Gebäuden installiert werden.

M 2.31 Einsatz mobiler Computer

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Betreiber, IT-Personal

Die Leiterinnen und Leiter der Einrichtungen und das IT-Personal müssen geeignete Maßnahmen (Handlungsanweisungen, Sicherheits- und Sicherungssoftware) veranlassen, um die Benutzerinnen und Benutzer beim Schutz mobiler Computer zu unterstützen (s. Maßnahme M 1.11). Es sind außerdem organisatorische und sicherheitstechnische Maßnahmen zu treffen, damit vom Einsatz mobiler Computer keine Gefährdungen für andere IT-Systeme ausgehen, insbesondere in Netzbereichen mit erhöhtem Schutzbedarf.

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

M 2.32 Einsatz von Diebstahl-Sicherungen

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragter
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 ergeben z. B. dort Sinn, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzerinnen bzw. 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.

Große Werte stellen auch Forschungsdaten und personenbezogene Daten dar. Datenträger mit solchen Daten sind deshalb in angemessener Weise zu schützen.

Zugriffsschutz

Grundsätzlich gilt, dass nur die Personen Zugang zum Netz und den damit verfügbaren Ressourcen der HU erhalten, die zuvor die Erlaubnis zur Nutzung von den dafür zuständigen Stellen erhalten haben. Jede Nutzungserlaubnis ist grundsätzlich personengebunden, d. h., anonyme Nutzerkonten sollten nur in begründeten Ausnahmefällen erlaubt werden (z. B. Zugang für FTP- oder WWW-Server, organisatorische Anforderungen).

In der Regel ist der Zugang zum Netz verbunden mit dem Zugriff auf Daten, Anwendungsprogramme und weitere Ressourcen. Daher hat die Authentisierung der Benutzerinnen und Benutzer des Netzes an jedem IT-System der HU eine besondere Bedeutung.

M 2.33 Personenbezogene Kennungen (Authentifizierung)

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

Es gelten die Hinweise unter Maßnahme M 1.16.

Die Einrichtung und Freigabe einer Benutzerkennung dürfen nur in einem geregelten Verfahren erfolgen. Sie sind zu dokumentieren.

M 2.34 Administratorkennungen

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

Das Verwenden von Benutzerkennungen mit weit reichenden 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.

M 2.35 Ausscheiden von Mitarbeitern

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen
Verantwortlich für Umsetzung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte

Verlässt eine Mitarbeiterin oder ein Mitarbeiter die Institution, wechselt die Funktion oder ändert sich das Tätigkeitsfeld, ist einerseits eine Übertragung sicherheitsrelevanter Aufgaben und Funktionen erforderlich, andererseits ist der Entzug der durch Wissen und Besitz eingeräumten Zutritts-, Zugangs- und Zugriffsrechte für IT-Systeme, IT-Verfahren oder Daten notwendig.

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass die bzw. der zuständige IT-Sicherheitsbeauftragte rechtzeitig über das Ausscheiden oder den Wechsel von Mitarbeiterinnen bzw. Mitarbeitern informiert wird. Die zuständige Leiterin bzw. der

zuständige Leiter hat über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung der jeweiligen Person zugeordnet sind. Vor dem Ausscheiden sind sämtliche Unterlagen, die sicherheitsrelevante Angaben enthalten, und ausgehändigte Schlüssel zurück zu fordern. Es sind sämtliche für die ausscheidende Person eingerichteten Zugangsberechtigungen und Zugriffsrechte zu deaktivieren bzw. zu löschen. Ggf. vorhandene Bezüge in Notfallplänen sind zu ändern. Vertretungsregelungen sind zu prüfen. 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.

M 2.36 Gebrauch von Passwörtern, Chipkarten, PINs, privaten Schlüsseln und Zertifikaten

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

Bei administrativen Zugängen auf IT-Systeme wird auf passwortloses zertifikatsbasiertes Arbeiten orientiert.

Es gelten die Hinweise unter Maßnahme M 1.17.

Darüber hinaus sind für IT-Systeme folgende Regeln einzuhalten:

- Wenn ein Passwort schriftlich fixiert wird (z. B. für die Hinterlegung zur Absicherung der personellen Vertretung), muss es gesichert aufbewahrt werden.
- Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr erneut verwendet werden.

Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- IT-Anwender müssen ihr eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer Anwender sollten Einmalpasswörter vergeben werden. Das sind Passwörter, die nach dem einmaligen Gebrauch gewechselt werden müssen.
- Bei der Authentifizierung in vernetzten Systemen sollten Passwörter 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.

M 2.37 Zugriffsrechte (Autorisierung)

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

Es gelten die Hinweise unter Maßnahme M 1.18.

Zugriffsrechte sind restriktiv zu vergeben. Für Personen mit besonderen Rechten, insbesondere für Administratorkennungen, ist eine Zugangsbegrenzung auf die notwendigen Computer (i.d.R. sind es der betreffende Server und die PCs der Serveradministratoren) einzurichten. 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.

M 2.38 Abmelden und ausschalten

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

Es gelten die Hinweise unter Maßnahme M 1.15.

Soweit es technisch möglich ist, sind zentral administrierte IT-Systeme so zu konfigurieren, dass die Maßnahmen unter M 1.15 umgesetzt werden und durch die Benutzerin bzw. den Benutzer nicht ohne weiteres deaktiviert werden können.

System- und Netzwerkmanagement

Die Absicherung des Zugriffs auf IT-Systeme sowie eine angemessene Protokollierung, Auditierung[6] und Revision ihrer Zugriffe sind wesentliche Faktoren der Netzsicherheit. Eine Auswertung solcher Protokolle (Logdaten) ist eine notwendige Hilfe beim Support und bei der Suche von Fehlern. Geeignete Auswertungen erlauben Rückschlüsse, ob Angriffe auf das Netz vorliegen und ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt.

Die Dauer der Speicherung und die Auswertung von Protokolldateien sind in Abhängigkeit von den Aufgaben der IT-Systeme und vom Zweck und Schutzbedarf der protokollierten Daten mit der bzw. dem behördlichen Datenschutzbeauftragten und ggf. der zuständigen Personalvertretung abzustimmen.

Mit Hilfe geeigneter Protokolle lässt sich feststellen, wer wann welche Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit). Je nach Schutzbedarf des Verfahrens müssen adäquate Maßnahmen zur Protokollierung getroffen werden, um die Revisionsfähigkeit zu gewährleisten. Bei der Revision werden die beim Audit gesammelten Daten von einem oder mehreren unabhängigen Mitarbeitern (4-Augen-Prinzip) überprüft, um Unregelmäßigkeiten beim Betrieb der IT-Systeme aufzudecken und ggf. auch die Arbeit der Administratoren zu kontrollieren.

Protokollierung, Auditierung und Revision sind im Sicherheitskonzept des IT-Systems zu regeln.

M 2.39 Protokollierung

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

Protokollierung ist in einem sinnvollen Umfang zu aktivieren. Es sollten alle sicherheitsrelevanten Ereignisse protokolliert werden. 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.

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 BlnDSG bzw. § 31 BDSG ist zu beachten. Keinesfalls sind Auswertungen erlaubt, die Rückschlüsse auf das Verhalten einzelner Personen zulassen.

---

[6] 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.

Wenn nicht anders festgelegt, sind Protokolldaten nach 8 Tagen zu löschen. Danach dürfen die aus Protokollen gewonnenen Daten z. B. für statistische oder Abrechnungszwecke nur anonymisiert und nach Zeit und Einrichtung aggregiert gespeichert werden.

M 2.40 Protokollierung durch Anwendungsprogramme

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

Bei der Protokollierung durch Anwendungssysteme ist der Grundsatz der Datenvermeidung nach § 3a BDSG zu beachten, d. h., die von Anwendungssystemen erzeugten Protokolldaten, die so wenig wie möglich personenbezogene Daten enthalten, sind vor dem Zugriff Unbefugter zu schützen. Es gelten die unter Maßnahme M 2.39 genannten Regeln entsprechend, insbesondere ist bei Daten mit Personenbezug das Zweckbindungsgebot zu beachten.

M 2.41 Protokollierung der Administrationstätigkeit

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragte
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, durchgeführte Änderungen an den IT-Systemen in einer Änderungshistorie (changelog) zu dokumentieren.

M 2.42 Monitoring von IT-Systemen

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

Server und andere IT-Systeme, auf ihnen laufende Prozesse und ihre Ressourcenausnutzung sollten nach Möglichkeit durch automatisch arbeitende Monitoring-Systeme überwacht werden. Dadurch sollen Betriebsprobleme frühzeitig erkannt werden. Die Probleme sind an die zuständigen Administratoren oder an Bereitschaftsdienste per E-Mail oder nach Möglichkeit per SMS zu signalisieren. Die notwendige personalrechtliche Absicherung ist zu beachten.

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-Anwender der Universität sind über die besonderen Risiken und Gefahren der elektronischen Kommunikation und der Datenübermittlung in Kenntnis zu setzen.

M 2.43 Sichere Netzwerkadministration

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

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.

M 2.44 Netzmonitoring

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

Es müssen geeignete Maßnahmen getroffen werden, um Überlastungen und Störungen im Netzwerk frühzeitig zu erkennen und zu lokalisieren. Es ist vergleichbar zu Maßnahme M 2.42 vorzugehen.

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.

M 2.45 Deaktivierung nicht benötigter Netzwerkzugänge

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

Es gelten die Hinweise unter Maßnahme M 1.19.

Ungenutzte Anschlussdosen an das Netz der HU sind in der Regel zu deaktivieren. Reservedosen, die an Switches angeschlossen sind, sind sparsam vorzuhalten.

Es sind Maßnahmen zu treffen, dass keine ungesicherten Anschlussdosen mit freiem Netzzugang in öffentlichen Bereichen zugänglich sind. Sie sind also in ihrer Nutzung einzuschränken, per Authentifizierung zu sichern oder zu deaktivieren.

M 2.46 Aufteilungen in Bereiche unterschiedlichen Schutzbedarfs

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Personal, IT-Betreiber

Das Datennetz ist so zu strukturieren, dass Teilnetze für verschiedene IT-Systeme entsprechend ihres jeweiligen Schutzbedarfs bereitgestellt werden. Bereiche mit hohem Schutzbedarf sind ggf. über die Standardmaßnahmen des CMS zur Gewährleistung der allgemeinen Netzsicherheit hinaus zusätzlich abzusichern. Systeme mit unterschiedlichem Schutzbedarf sollten nicht in gleichen Teilnetzen betrieben werden. Dadurch wird verhindert, dass Systeme mit hohem Schutzbedarf durch zu wenig gesicherte Systeme im gleichen Teilnetz oder ungenügende Schutzmaßnahmen an Netzübergängen gefährdet werden. Umgekehrt wird damit aber auch erreicht, dass die Nutzung von Systemen mit geringerem Schutzbedarf nicht unnötig erschwert wird, weil auf andere Systeme mit höherem Schutzbedarf im gleichen Teilnetz Rücksicht genommen werden muss.

M 2.47 Kontrollierte Kommunikationskanäle

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

Die Kommunikation zwischen Netzbereichen mit unterschiedlichem Schutzbedarf oder mit externen Partnern darf ausschließlich über kontrollierte Kanäle erfolgen, die durch spezielle Schutzsysteme (Firewall, VPN-Gateway o. ä.) geführt werden. Die Regeln der Schutzsysteme sollten so definiert werden, dass unnötige Kommunikationen unterbunden werden und somit Angriffsflächen minimiert werden.

Die Einrichtung von Kommunikationskanälen zwischen Teilnetzen der HU sowie zu externen Netzen erfolgt durch den Betreiber des Netzes der HU (CMS) bzw. muss durch diesen genehmigt sein.

Datensicherung

M 2.48 Organisation der Datensicherung

Verantwortlich für Initiierung: Leiter/innen der Einrichtung, Verantwortliche für Datensicherungssysteme
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).

M 2.49 Datensicherung – Information und Durchführung

Verantwortlich für Initiierung: Verantwortliche für Datensicherungssysteme
Verantwortlich für Umsetzung: IT-Personal

Es gelten die Hinweise unter Maßnahme M 1.21.

Alle Administratoren und Anwender von IT-Systemen, die Datensicherungssysteme nutzen oder nutzen können, sollten über die Regelungen zur Datensicherung und über ihre Pflichten zur Verifizierung der durchgeführten Backups genau informiert werden. Sie müssen in der Lage sein, Risiken oder Unzulänglichkeiten für ihre Systeme zu erkennen. Die Informationen müssen auch Angaben zu ungefähren Wiederherstellungszeiten von Dateien oder gesamten Datenträgern enthalten.

Die Datensicherung von Servern erfolgt im Rahmen der verfügbaren Ressourcen turnusmäßig durch den CMS.

M 2.50 Verifizierung der Datensicherung

Verantwortlich für Initiierung: Verantwortliche für Datensicherungssysteme
Verantwortlich für Umsetzung: IT-Personal

Die Betreiber der zu sichernden IT-Systeme müssen nach einer Einrichtung bzw. Änderung der die Datensicherung bestimmenden Konfigurationsdateien prüfen, ob bei der darauf folgenden Datensicherung die zu sichernden Verzeichnisse bzw. Dateien wie beabsichtigt gesichert wurden.

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

Die Betreiber der Datensicherungssysteme müssen anhand der Log-Dateien prüfen, ob alle Daten, für die eine Sicherung eingerichtet wurde, vollständig gesichert wurden.

Datenträger

M 2.51 Umgang mit Datenträgern

Verantwortlich für Initiierung: Leiter/innen der Einrichtungen, IT-Sicherheitsbeauftragte
Verantwortlich für Umsetzung: IT-Personal

Es gelten die Hinweise unter den Maßnahmen M 1.22 und M 1.23.

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. Die Verfügbarkeit von Lesegeräten für die Dauer der Speicherung muss abgesichert sein.

Anlage 3 Glossar

Einrichtungen der HU

Einrichtungen der HU sind z. B. Fakultäten, Institute, Zentralinstitute, Graduate Schools, Interdisziplinäre Zentren, Integrative Forschungsinstitute, Zentraleinrichtungen und die Universitätsverwaltung.

IT

Informationstechnologie

IT-Infrastruktur der HU

Gesamtheit der Rechnernetze, Computerhardware, Computersoftware, IT-Anwendungssysteme und Peripherie, die an der HU zum Einsatz gebracht wird bzw. werden soll – darunter auch mobile Computer einschließlich Smartphones, vernetzte Computer in Steuerungs- und Regelungssystemen (embedded systems) sowie virtualisierte Systeme

IT-Personal

Zum IT-Personal der HU gehören IT-Systemverantwortliche, IT-Systemadministratoren, DV-Beauftragte, IT-Sicherheitsbeauftragte, Verantwortliche für IT-Anwendungen und IT-Verfahren.

IT-Systeme

IT-Systeme im Sinne dieser Richtlinie sind Hardware und/oder Software, IT-Verfahren und IT-Anwendungen die IT-Dienste anbieten. Beispiele sind: Datennetze, Speichernetze, Server, Client-Server-Systeme, IT-Anwendungen in Einrichtungen der HU

Anlage 4 Quellenverzeichnis

[1] BSI-Standard 100-1: Managementsysteme für Informationssichergeit (ISMS), Version 1.5, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001.pdf

[2] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002.pdf

[3] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003.pdf

[4] BSI-Standard 100-4: Notfallmanagement, Version 1.0, BSI 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004.pdf

[5] IT-Grundschutz-Kataloge, Stand 12. Ergänzungslieferung, BSI 2011
https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf

[6] Leitfaden Informationssicherheit: IT-Grundschutz kompakt, BSI 2009
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf