Freie Universität Berlin

Handlungsleitfaden für den Betrieb eines sicheren IT-Arbeitsplatzes für wissenschaftliches Arbeiten

Freie Universität Berlin

Version 1.1

21. Februar 2013

Steckbrief

Zielsetzung:	Konzept eines sicheren Arbeitsplatzes für wissenschaftliches Arbeiten
Regelungsinhalte:	Empfehlungen zur Bereitstellung eines sicheren wissenschaftlichen Arbeitsplatzes mit dem entsprechenden Service
Zielgruppe:	Mitarbeiter in der Forschung und Lehre, Bereichsleiter, IT-Beauftragte
Geltungsbereich:	Alle Einrichtungen der Freien Universität Berlin
Gültigkeitsdauer:	Unbegrenzt

Autoren

Mitglieder der AG IT-Sicherheit

Hr. Camphausen (FB Mathematik u. Informatik)
Hr. Dräger (eAS)
Fr. Heinau (ZEDAT)
Fr. Pahlen-Brandt (DS)
Hr. Posel (FB Geschichts- und Kulturwissenschaften)
Hr. Dr. Sommerer (FB Veterinärmedizin)
Fr. Dr. Wittkopf (FB Rechtswissenschaft)
Hr. Dr. Woidt (FB Physik)
Hr. Worch (FB Biologie, Chemie, Pharmazie)

Beraten im CIO-Gremium und abgestimmt mit dem FIT-Gremium, der Personalvertretung, den Datenschutzbeauftragten und den IT-Beauftragten.

Inhaltsverzeichnis

Zusammenfassung

Ziel des Konzepts ist ein sicherer IT-Arbeitsplatz für wissenschaftliches Arbeiten. Die nachhaltige Gewährleistung eines Mindeststandards von Informationssicherheit und Datenschutz kann erfahrungsgemäß nur durch einen zentral administrierten Arbeitsplatzrechner[1] erreicht werden. Damit das alltägliche Arbeiten ohne besondere Privilegien (Administratorrechte) von den Wissenschaftlern akzeptiert und nicht als „Verzicht“ empfunden wird, muss dieser Arbeitsplatzrechner ein schnelles und flüssiges Arbeiten ermöglichen. Unabdingbare Voraussetzung hierfür ist ein gut funktionierender IT-Service. Ein selbst administrierter Arbeitsplatzrechner ist bei bestimmten Anforderungen möglich. Die Selbstadministration erfordert eine stetige zeitnahe Pflege des Systems und damit auch einen eingewiesenen kompetenten Nutzer.

[1] Die zentrale Administration kann durch geeignete Stellen universitätszentral oder dezentral, beispielsweise auf Ebene eines Fachbereichs, Zentralinstituts oder zentraler Einrichtung, erfolgen. Häufig ist die in diesem Dokument benannte zentrale Administration eine sich ergänzende Mischform aus zentralen und dezentralen Services.

1 Geltungsbereich

Die in dem Konzept eines sicheren IT-Arbeitsplatzes für wissenschaftliches Arbeiten skizzierten Empfehlungen sollen in allen Einrichtungen der Freien Universität Berlin umgesetzt werden.

2 Anforderungen

Anforderungen an den Betrieb eines sicheren Arbeitsplatzes für wissenschaftliches Arbeiten ergeben sich aus den Erwartungen der Wissenschaftler sowie aus technischen Gegebenheiten der IT-Sicherheit. Im Folgenden werden zunächst die Erwartungen der Wissenschaftler beschrieben (2.1), anschließend die Anforderungen aus Sicht der Informationssicherheit (2.2). Datenschutzaspekte finden sich in beiden Gruppen; sie sind nicht besonders als Datenschutzanforderungen ausgewiesen.

2.1 Erwartungen des Wissenschaftlers

Aus der Sicht des Wissenschaftlers stellt die IT bzw. ein Arbeitsplatz-Computer ein Werkzeug dar, das zuverlässig funktionieren muss:

- Installation benötigter, noch nicht installierter Software in kurzer Zeit
- Schutz vor fremden Zugriff auf die Daten
- Wiederherstellung verlorener Daten
- Archivierung von Forschungsdaten
- Zuverlässige Verfügbarkeit des Rechners, insbesondere wenn dieser Teil eines wissenschaftlichen Experiments ist (z. B. Messrechner)
- Zugriffsmöglichkeit auf ältere Versionen von Dokumenten, Daten und Programmen
- Bereitstellung von Informationsmaterial
- Erreichbarkeit eines Ansprechpartner in IT-Fragen
- Mobile Geräte[2] müssen in unterschiedlichen Netzen und Standorten funktionsfähig sein

2.2 Anforderungen aus Sicht der IT-Sicherheit

- Zentral administrierte Rechner
  Erläuterung: Um die Arbeitsplatzrechner stets mit aktuellen Patches versorgen zu können, zur Gewährleistung einer sicheren Grundkonfiguration und zur schnellen Behebung von Störungen ist eine zentrale Administration notwendig.
- Alltägliche Rechnernutzung ohne besondere Privilegien; Administratorrechte bei technischer Notwendigkeit
  Erläuterung: Damit bei einem möglichen Missbrauch, z. B. durch Schadprogramme oder durch eine missbräuchliche Account-Nutzung, der Wirkungsbereich möglichst begrenzt bleibt, darf nur mit besonderen Rechten gearbeitet werden, wenn die Erfüllung der Aufgabe dies erfordert.

[2] Mobile Geräte im Sinne dieses Konzepts sind IT-Systeme, die als wissenschaftlicher Arbeitsplatz genutzt werden können.

- Trennung von System und Daten
  Erläuterung: Damit die Daten zuverlässig und einfach gesichert und wiederhergestellt werden können, ist eine Trennung von Programm- und Betriebssystemdateien notwendig. Beispielsweise kann den Benutzern für die Datenablage ein RAID-5-Netzlaufwerk zur Verfügung gestellt werden. Dadurch ist auch die Wahrscheinlichkeit geringer, dass sich Fehler bei Arbeiten am System negativ auf die gespeicherten Daten auswirken.
- Separate Netze für spezielle Anforderungen (Beispiel: Messrechner mit veraltetem Betriebssystem)
  Erläuterung: Wenn mit systemeigenen Mitteln die Sicherheit nicht gewährleistet werden kann (weil z. B. das Betriebssystem nicht mehr mit Sicherheits-Patches versorgt werden kann), müssen die gefährdeten Systeme netztechnisch separiert werden.
- Firewall (geschützte Netze)
  Erläuterung: Als Schutz vor unberechtigtem Zugriff kann die Erreichbarkeit der Rechner begrenzt und kontrolliert werden.
- Sichere Authentifizierung (persönliche Accounts)
  Erläuterung: Eine sichere Authentifizierung mit einem persönlichen Account ist eine Grundvoraussetzung zur IT-Sicherheit, insbesondere zum Schutz der Daten vor unberechtigtem Zugriff.
- Rollentrennung und Berechtigungssteuerung (Autorisierung)
  Erläuterung: Eine revisionssichere Autorisierung (Protokollierung) gehört zu den Grundvoraussetzungen der Informationssicherheit und des Datenschutzes.
- Verschlüsselung von Daten mit hohem Schutzbedarf
  Erläuterung: Zur Gewährleistung der Vertraulichkeit und auch der Integrität sollten Daten mit hohem Schutzbedarf verschlüsselt werden. Daten mit sehr hohem Schutzbedarf oder Daten, die der Geheimhaltung unterliegen, müssen in der Regel verschlüsselt werden.
- Mobile Arbeitsplatzrechner, deren Pflege- und Wartungszustand ungeklärt ist, müssen vor dem Anschluss an ein FU-Netz überprüft werden
  Erläuterung: Damit ein mobiler Rechner den Status „sicherer Arbeitsplatz“ erlangen kann, muss mindestens sichergestellt werden, dass auf dem mobilen Rechner alle relevanten Sicherheits-Patches installiert und eine Prüfung auf „Virenbefall“ erfolgreich durchlaufen wurde.
- Datenschutz
  Erläuterung: An der Freien Universität Berlin werden die Ziele des Datenschutzes und der Informationssicherheit gleichberechtigt und als sich ergänzende Bausteine einer Gesamtsicherheitsbetrachtung behandelt. Daher unterscheiden sich personenbezogene Daten von anderen Daten nur insofern, als sie aufgrund dieser Eigenschaft bereits schutzwürdig sind.
- Schulung der wissenschaftlichen Mitarbeiter
  Erläuterung: IT-Benutzer müssen über die wichtigsten Aspekte der Informationssicherheit und des Datenschutzes informiert werden.
- Bereitstellung von Informationsmaterial zum sicheren IT-Einsatz
  Erläuterung: Zur Unterstützung der selbstständigen Arbeit des betreffenden Mitarbeiters und als flankierende Maßnahme einer Schulung wird In-

formationsmaterial benötigt. Vorrangig wird über die Notwendigkeit von Schutzmaßnahmen sowie über die relevanten Bestimmungen der IT-Sicherheitsrichtlinie informiert. Ein gutes Beispiel dafür sind die jeweils relevanten ZEDAT-Anleitungen (Tip4U) sowie die einschlägigen Informationsflyer („Praxistipps zur IT-Sicherheit“ und „Regelwerke für den IT-Einsatz“).

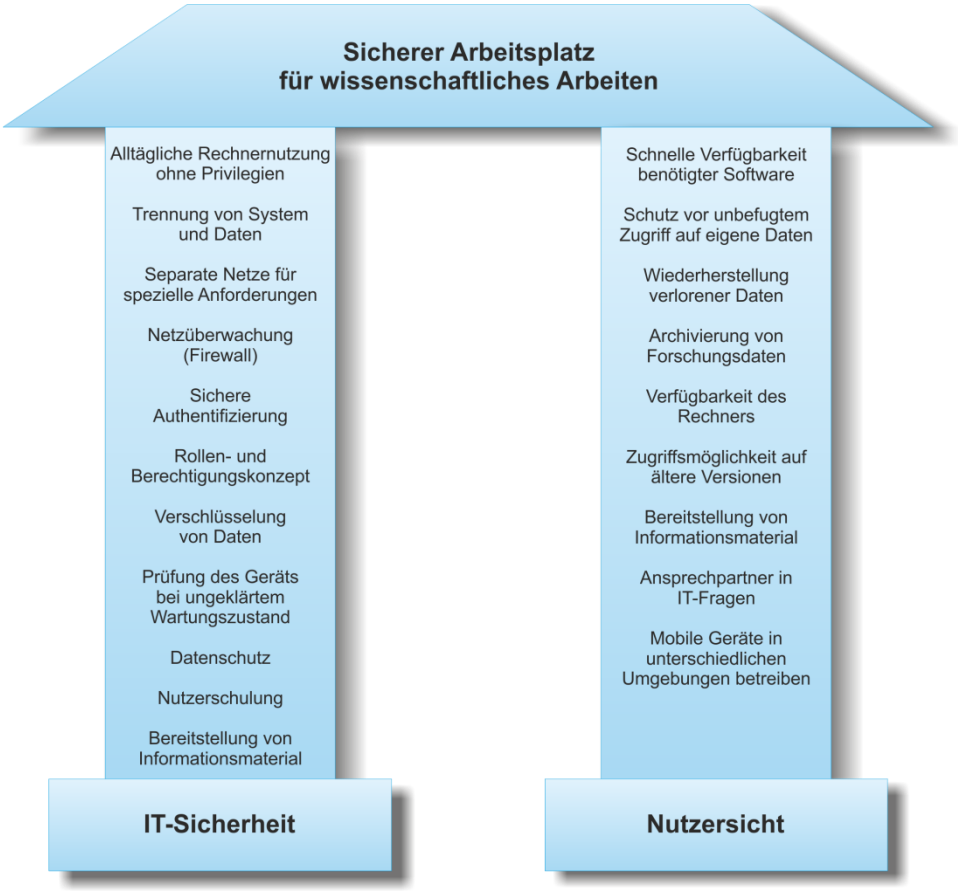

Abbildung 1: Veranschaulichung der Anforderungen der IT-Sicherheit und der Erwartungen des Nutzers (Nutzersicht) als zwei Säulen, auf denen das abgestimmte Konzept eines sicheren wissenschaftlichen Arbeitsplatzrechners ruht.

2.3 Folgerungen

→ Grundausstattung mit IT-Personal / Betreuungspersonal

Erläuterung: Um einen umfassenden Service mit kurzen Reaktionszeiten anbieten zu können, bedarf es einer adäquaten personellen Grundausstattung.

3 Konzept

Ein Konzept für einen sicheren wissenschaftlichen Arbeitsplatz muss das Spannungsfeld zwischen Sicherheitsanforderungen und größtmöglicher Freiheit des wissenschaftlichen Arbeitens nicht nur berücksichtigen, sondern auch auflösen. Dieses Konzept soll die Gegensätze so austarieren, dass den Wissenschaftlern ein sicherer IT-Arbeitsplatz zur Verfügung gestellt werden kann, der die Freiräume wissenschaftlichen Arbeitens nicht beeinträchtigt.

Bei einem wissenschaftlichen Arbeitsplatz kann nicht von dem Einsatz immer gleicher Software ausgegangen werden. In Abhängigkeit von der wissenschaftlichen Disziplin und dem konkreten Betätigungsfeld kommt eine große Vielfalt von unterschiedlichen Programmen zum Einsatz. Eine Einschränkung der (computergestützten) Kommunikation ist im wissenschaftlichen Umfeld weder praktikabel noch wünschenswert.

3.1 Kernelemente des Konzepts

Das im Folgenden vorgestellte Konzept basiert auf zentral verwalteten Arbeitsplatzrechnern. Die zentrale Verwaltung kann entweder im Hochschulrechenzentrum und/oder im jeweiligen Fachbereich erfolgen. Ein selbstadministrierter Rechner ist bei bestimmten operativen Anforderungen möglich, wie beispielsweise bei Nutzung von privaten Geräten für dienstliche Aufgaben. Das Konzept besteht aus den folgenden Kernelementen und den sich daraus ergebenen Konsequenzen:

Kernelement 1:	**Zentral administrierte Computer**
Folgerung 1.1:	Der Nutzer (Wissenschaftler) arbeitet grundsätzlich ohne Administratorrechte.
Folgerung 1.2:	Bereitstellung zentraler Services, wie Datensicherung, Virenschutz, Patch-Management für alle eingesetzten Programme, Help Desk, IT-Support.
Folgerung 1.3:	Die verfügbare Hard- und Software genügt den wissenschaftlichen Anforderungen.
Folgerung 1.4:	Auf Installations- und Konfigurationswünsche der Nutzer wird schnell reagiert.
Folgerung 1.5:	Eine den wissenschaftlichen Anforderungen genügende Softwareauswahl ist schnell verfügbar (z. B. als Self Service).

Kernelement 2:	**Abweichende Reglungen**
Folgerung 2.1:	Wenn Computer nicht hinreichend abgesichert werden können (weil z. B. ein spezielles Messprogramm nur auf einem alten Betriebssystem läuft), müssen andere Maßnahmen (z. B. ein separates und geschütztes Netzsegment) die Sicherheit gewährleisten.
Folgerung 2.2:	Wissenschaftliche Mitarbeiter, die aufgrund ihrer Kenntnisse und ihres Aufgabengebiets Administrations- oder Softwareentwicklungsarbeiten wahrnehmen, werden als IT-Personal betrachtet und unterliegen in dieser Rolle den Weisungen der jeweiligen IT-Leitung (IT-Leiter vor Ort, IT-Beauftragter oder andere Stelle).

Folgerung 2.3:	Administratorrechte können an versierte Nutzer temporär vergeben werden, damit beispielsweise auf Exkursionen Einstellungen geändert oder Reparaturen selbst durchgeführt werden können. Diese Rechte dürfen nur bedarfsweise im Einzelfall genutzt werden.
Folgerung 2.4:	Bei selbst administrierten Computern muss der Nutzer die Übernahme der Verantwortung für den dauerhaft selbst administrierten Rechner mit seiner Unterschrift bestätigen. Ein Formular als Beispiel befindet sich im Anhang.

Kernelement 3:	**Transparenz**
Folgerung 3.1:	Die Umsetzung des Konzepts, wie zum Beispiel Informationen über Kontaktdaten des IT-Supports, Datensicherungszyklen und das Procedere der Bereitstellung von Software ist verständlich dargestellt.

Kernelement 4:	**Mobile Geräte**
Folgerung 4.1:	Mobile Geräte, die als IT-Arbeitsplatz für wissenschaftliches Arbeiten genutzt werden, sollten – soweit wie möglich – zentral administriert.
Folgerung 4.2:	Der Zugriff auf FU-Ressourcen erfolgt nur über verschlüsselte und authentisierte Kanäle.
Folgerung 4.3:	Die Regelungen der IT-Sicherheitsrichtlinie werden bei der Speicherung schützenswerter Daten beachtet (z. B. Pflicht zur Verschlüsselung).

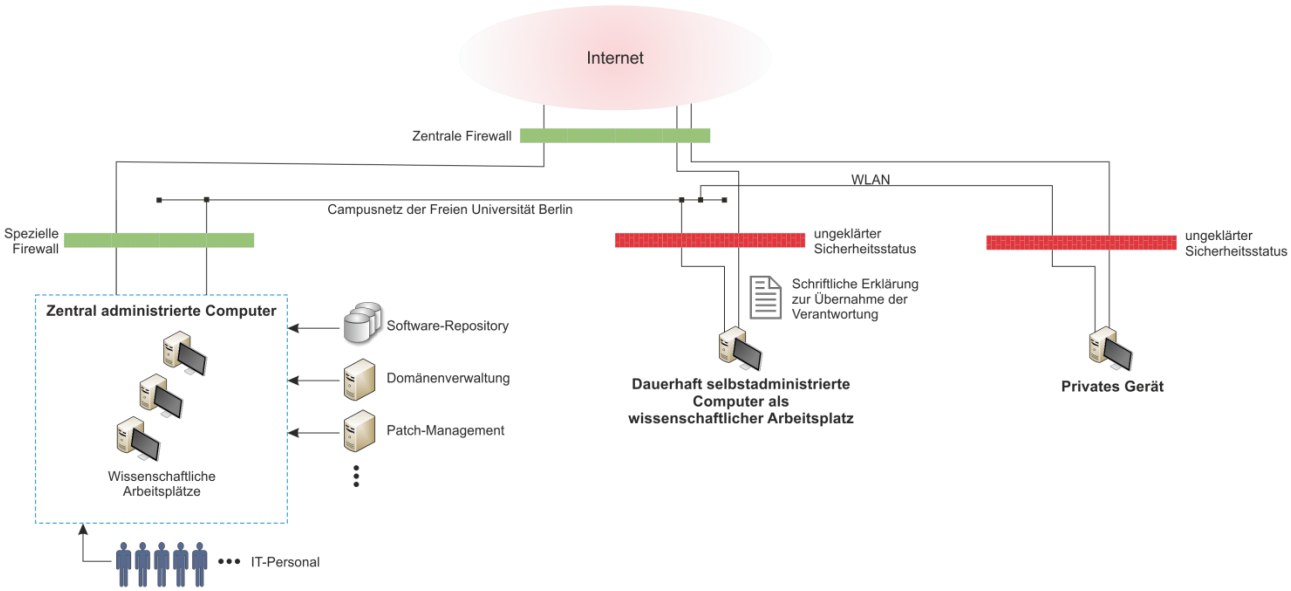

Abbildung 2: Gegenüberstellung von zentral administrierten und selbstadministrierten Rechnern.

3.2 Umsetzung des Konzepts

Ein zentrales Element des IT-Services für Wissenschaftler ist die Attraktivität der Dienstleistung. Das wird erreicht durch hohe Flexibilität, mit der auf Nutzerwünsche reagiert werden kann. Idealerweise sollte hierfür sowohl vor Ort IT-Personal zur Verfügung stehen, als auch ergänzend IT-Personal in den zentralen IT-Bereichen (ZEDAT, CeDiS, eAS, UB). Auf Grund der spezifischen Anforderungen, die sich aus der wissenschaftlichen Disziplin und dem Forschungsgebiet ergeben, sollte IT-Personal auch in den dezentralen wissenschaftlichen Einrichtungen vorhanden sein, damit auf spezielle Anforderungen schnell und adäquat reagiert werden kann.

Das IT-Personal des zentralen Hochschulrechenzentrums und der dezentralen Einrichtungen arbeitet so zusammen, dass ein für den Nutzer transparenter, hochwertiger Service geboten wird.

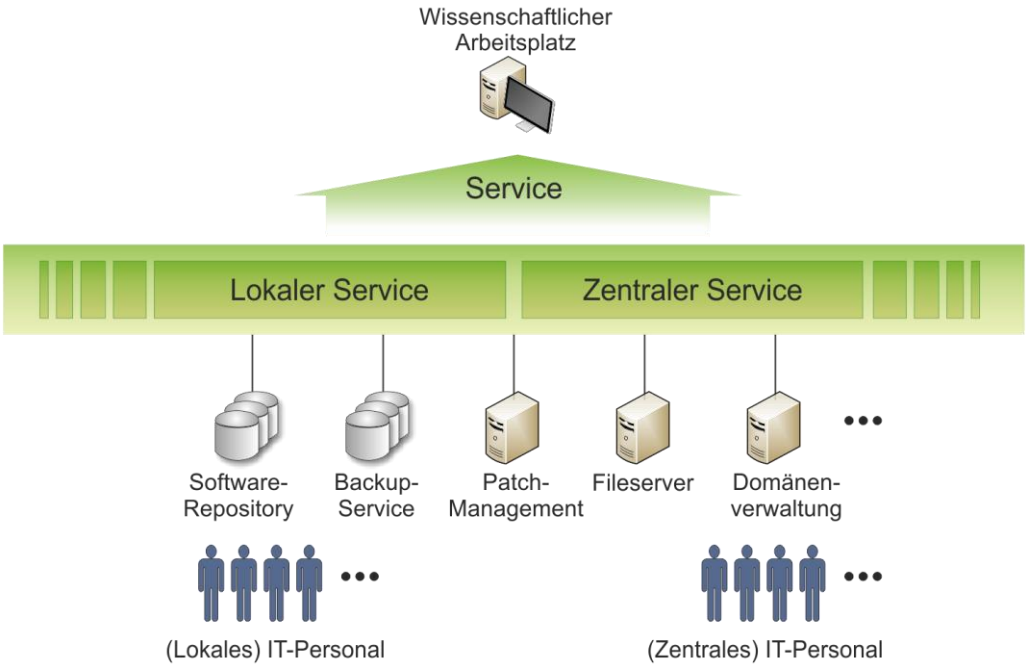

Abbildung 3: Skizze eines Services, der gemeinsam von zentralen und dezentralen IT-Einrichtungen erbracht wird.

4 Musterverfahren zur Selbstadministration

Die Freie Universität Berlin ist bestrebt Ihren Mitgliedern auch für wissenschaftliches Arbeiten zentrale Administration für sichere Arbeitsplätze anzubieten. Eine Selbstadministration kann in Einzelfällen erforderlich und zulässig sein. In jedem Fall sind die in den Sicherheitsrichtlinien der Freien Universität Berlin beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden für alle Einrichtungen der Freien Universität Berlin verbindlich.

Die Freischaltung eines selbstadministrierten Rechners im Netz der Freien Universität Berlin erfordert das Einverständnis des Leiters des Arbeitsbereiches, der verantwortlich ist für den ordnungsgemäßen Betrieb des selbstadministrierten Rechners und die Einhaltung der Regeln zur IT-Sicherheit. Darüber hinaus ist die Zustimmung durch die zuständige IT-Stelle erforderlich.

Für selbstadministrierte Rechner besteht kein Anspruch auf Support durch die ansonsten zuständigen IT-Dienste der Freien Universität. Im Falle der Nichteinhaltung der Bestimmungen kann der Rechner unverzüglich vom FU-Netz getrennt.

4.1 Mustererklärung

Erklärung zum Betrieb eines selbstadministrierten Rechners im Netz der Freien Universität Berlin

Die in den Sicherheitsrichtlinien beschriebenen organisatorischen, personellen, technischen und infrastrukturellen Maßnahmen und Methoden sind für alle Personen verbindlich, die IT-Ressourcen der Freien Universität Berlin nutzen. Sie sind als PDF-Datei auf den Webseiten der Freien Universität Berlin abrufbar[3].

Die Unterzeichnenden erklären, die IT-Richtlinien zu kennen und einzuhalten.

Im Besonderen bedeutet dies:

- Der Leiter des Arbeitsbereichs benennt einen Mitarbeiter (oder sich selbst), der die Verantwortung für den ordnungsgemäßen Betrieb des selbstadministrierten Rechnersystems trägt und die Einhaltung der Regeln der IT-Sicherheitsrichtlinie garantiert. Bei Urlaub oder Abwesenheit ist ein Vertreter zu bestimmen.
- Für selbstadministrierte Rechner besteht kein Anspruch auf Support durch die ansonsten zuständigen IT-Mitarbeiter.
- Es gibt für den Nutzer genau einen Account mit Administratorrechten, der ausschließlich für spezielle Zwecke (Installation von Software, Änderungen von Systemeinstellungen, systemnahe Programmierung usw.) genutzt werden darf.
- Für die normale Nutzung des Rechners arbeitet jeder Nutzer mit einem persönlichen Account, der keine besonderen Privilegien hat.
- Wahl eines sicheren Passworts nach den Regelungen der IT-Sicherheitsrichtlinie der Freien Universität Berlin.
- Installation eines Virenscanners, der sich über das Netz selbst aktualisiert. Allen Mitgliedern der FU steht der Virenscanner von McAfee kostenlos zur Verfügung.
- Updateservices dürfen nicht abgeschaltet werden.
- Lokale Firewall-Systeme müssen aktiviert sein.
- Im Fall von Missbrauch wird der entsprechende Rechner unverzüglich vom FU-Netz getrennt.

Identifikation des Rechners: (DNS-Name, Inventarnummer o. ä.)	

Name des Leiters des Arbeitsbereichs	*Unterschrift*	Berlin, den	*Datum*
Name des verantwortlichen Ansprechpartners für diesen Rechner	*Unterschrift*	Berlin, den	*Datum*
Name des zuständigen IT-Beauftragten	*Unterschrift*	Berlin, den	*Datum*

[3] http://www.fu-berlin.de/sites/eas/it-sicherheit/FU-Regelwerke/index.html

5 Weitere Informationen

- Alle universitätsinternen IT-Regelwerke stehen auf den folgenden Webseiten zur Verfügung:

  http://www.fu-berlin.de/sites/it-sicherheit/

  http://www.fu-berlin.de/sites/eas/it-sicherheit/FU-Regelwerke/index.html

- Das Hochschulrechenzentrum (ZEDAT) bietet eine Sammlung nützlicher Merkblätter – "Tip4U" – an, die ausgewählte Themen aus dem IT-Bereich behandeln und die Nutzung der ZEDAT-Dienste mit bebilderten Anleitungen veranschaulichen:

  http://www.zedat.fu-berlin.de/Tip4U

- Der erste Ansprechpartner in allen IT-Fragen ist der IT-Beauftragte der jeweiligen Einrichtung. Eine Liste der IT-Beauftragten steht unter der folgenden Webseite zur Verfügung:

  http://www.fu-berlin.de/IT-Beauftragtenliste

- Regelungen und Hinweise zu sozialen Netzwerken an der Freien Universität Berlin sind in der Richtlinie „Grundregeln zur offiziellen Verwendung von sozialen Netzwerken durch Einrichtungen und Mitarbeiter/innen der Freien Universität Berlin“ festgelegt.

  http://www.fit.fu-berlin.de/it-richtlinien/social_web/index.html