Beim **Anschluss von IT-Systemen an das Netz der Freien Universität Berlin** sind eine Reihe von bereichsübergreifenden Maßnahmen und Regelungen einzuhalten. Eine Auswahl der wichtigsten Regelungen wurde in diesem Dokument übersichtsartig zusammengefasst. Grundsätzlich sind jedoch alle in der IT-Sicherheitsrahmenrichtlinie definierten Grundschutzmaßnahmen sowie die Regelungen der ZEDAT-Benutzungsordnung und die Campusnetz-Policy zu beachten.

Benutzungsordnung und Campusnetz-Policy der ZEDAT

Die Zulassung zur Inanspruchnahme von Dienstleistungen der ZEDAT erfolgt auf Antrag. In den Anträgen sind Art und Umfang der beabsichtigten Nutzung sowie ggf. besondere Leistungen, die eine spezielle Geräteeinrichtung benötigen, anzugeben. Der Benutzer verpflichtet sich, die IT-Komponenten sachgerecht zu behandeln, Schäden, Störungen und Fehler unverzüglich dem Personal der ZEDAT sowie die Verarbeitung personenbezogener Daten der ZEDAT mitzuteilen. Der Benutzer hat jeden unerlaubten Zugriff auf Daten, insbesondere Einsichtnahme, Veränderung oder Löschung zu unterlassen. Die Einhaltung der einschlägigen Rechtsvorschriften, insbesondere des Datenschutzes, ist sicherzustellen.

Zu den wichtigsten Punkten der Campusnetz-Policy gehören die Hinweise zu Nameservereinträgen, die Pflicht zur Eintragung von Rechnern im Domain Name System (DNS), die Möglichkeit zur eindeutigen Identifizierung eines Rechners im Missbrauchsfall und damit die Einschränkung der Nutzung von dynamisch zugewiesenen IP-Adressen über DHCP sowie der Schutz von Netzwerkdosen in öffentlich zugänglichen Räumen vor missbräuchlicher Nutzung.

Dokumentation

Zu jedem IT-System ist eine Dokumentation zu führen. Die Dokumentation muss mindestens den Aufstellungsort und Unterlagen zur Hard- und Softwareausstattung, Garantieleistungen, Wartungsverträgen, Lizenzen usw. enthalten. Darüber hinaus sind weitere Angaben, die in den Grundschutzmaßnahmen konkretisiert sind, zu dokumentieren.

Der gesamte IT-Einsatz wird vom IT-Verantwortlichen in IT-Verfahren gruppiert. Jedes IT-Verfahren ist nach den Vorgaben der IT-Sicherheitsrahmenrichtlinie zu beschreiben. Die IT-Verfahren sind zusätzlich bezüglich der Sicherheit zu dokumentieren. Nur dokumentierte IT-Verfahren dürfen betrieben werden. Der IT-Verantwortliche sorgt für die aktuelle Dokumentation der IT-Verfahren seines Bereiches. Er ist verantwortlich für die Erstellung und Pflege der Dokumentation der IT-Verfahren seines Bereiches. Verfahrensverantwortliche, Systemadministratoren und Applikationsbetreuer sind dabei durch die IT-Organisationsrichtlinie zur Mitarbeit verpflichtet.

Sicherung der Computer-Hardware

Der unbefugte Zugang zu Geräten und die Benutzung der Informationstechnik muss verhindert werden. Bei Abwesenheit sind Mitarbeiter-Räume mit IT verschlossen zu halten. Es muss gewährleistet sein, dass Schlüssel nur an die jeweils berechtigten Personen ausgegeben werden. Bei der Anordnung und baulichen Einrichtung der Geräte ist darauf zu achten, dass Daten mit internem oder vertraulichem Inhalt nicht von Unbefugten eingesehen werden können. Diebstahl-Sicherungen für Endgeräte 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.

Bei der Speicherung von schützenswerten Daten auf mobilen Computern (Notebooks) sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Derartige Daten müssen verschlüsselt werden. Notebooks sind möglichst verschlossen aufzubewahren.

Virenschutz

Auf allen Arbeitsplatz-PCs ist, soweit technisch möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Durch den Einsatz von Virenschutzsystemen soll das Eindringen von schädlichem Programmcode erkannt und verhindert werden. Regelmäßig (möglichst automatisiert) sind die Virenerkennungsmuster zu aktualisieren. Wird auf einem System schädlicher Programmcode entdeckt, muss dies der zuständigen Stelle gemeldet werden. Empfehlens-

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

Einsatz von Hard- und Software

Die Benutzung von privater Hard- und Software in Verbindung mit technischen Einrichtungen der Freien Universität Berlin und deren Netzen ist nicht gestattet. Ausgenommen von dieser Regelung sind speziell für den Einsatz privater Computer gekennzeichnete Bereiche. Der Anschluss von Systemen an das Datennetz der Freien Universität Berlin hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems o.ä.) ohne Absprache mit dem IT-Verantwortlichen des Bereichs ist unzulässig. Der Betrieb von Access-Points darf nur in Absprache mit der ZEDAT erfolgen.

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

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

Autorisierung

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

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

Meldepflicht

Auftretende Sicherheitsprobleme aller Art (Fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Eindringen Unbefugter, Manipulationen u.ä.) sind dem zuständigen IT-Personal mitzuteilen. Jeder schwerwiegende Vorfall ist zu dokumentieren.

Kommunikation zwischen unterschiedlichen Sicherheitsniveaus

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

Einsatz von IT-Personal

Die Auswahl und der Einsatz von IT-Personal müssen nach verschiedenen Kriterien erfolgen. Insbesondere mit Administrationsaufgaben auf Netzwerk- und Systemebene dürfen nur ausgewählte, ausreichend qualifizierte, vertrauenswürdige und motivierte Mitarbeiter betraut werden. Kurzzeitig befristet beschäftigte Mitarbeiter (Beschäftigungsverhältnis von weniger als einem Jahr) sollten nach Möglichkeit keine Aufgaben übernehmen, die nur mit Administratorrechten ausgeführt werden können. Daneben erfordert eine zuverlässige und sichere Erfüllung der IT-Aufgaben auch eine angemessene Personalausstattung.