



Kanzler

Dienstanweisung über den Umgang mit der IT-Technik der Verwaltung und des Rektorates der Martin-Luther-Universität Halle-Wittenberg

vom 23.09.2009

§ 1 Geltungsbereich und Gegenstand

(1) Die Dienstanweisung für die IT-Technik gilt für die Mitarbeiterinnen und Mitarbeiter (im folgenden Nutzer genannt) der Zentralen Universitätsverwaltung und des Rektorats.

(2) Die Dienstanweisung soll als Hilfestellung und Richtschnur für den Umgang mit der IT-Technik dienen. Soweit den Nutzern Bedienungsanleitungen für die einzelnen Geräte und Programme zur Verfügung stehen, sind diese zu beachten. Sollten Fragen und Probleme bei der Bedienung der Geräte oder Programme auftreten, die von den Nutzern nicht gelöst werden können, stehen die zuständigen Mitarbeiter der Abteilung 5 / Referat 5.2 zur Hilfeleistung zur Verfügung.

(3) Diese Regeln erstrecken sich auf folgende Geräte und Gerätekomponenten der IT-Technik: Personalcomputer oder Laptop bzw. Notebook (im folgenden Rechner genannt) mit folgenden möglichen Komponenten:

- Tastatur,
- Maus,
- Monitor,
- Drucker (soweit lokal vorhanden),
- Scanner (soweit vorhanden),
- andere Zusatzgeräte (soweit vorhanden),
- Netzwerkgeräte (Netzdrucker u.ä.).

Ausdrücklich nicht betroffen von dieser Regelung sind alle IT-Komponenten, die von Ref. 5.2 als Server betrieben werden und in zentralen Maschinenräumen installiert sind. Dies gilt ebenso für alle Netzwerkkomponenten (z. B. Firewalls, Switches o. ä.).

§ 2 Hardware

(1) Rechner und alle weitere IT-Technik der ZUV und des Rektorates werden nur vom Ref. 5.2 beschafft und installiert. Änderungen an der IT-Technik sowie Eingriffe in die Rechner und deren Komponenten, auch bei USB-Speichermedien, dürfen nur von den zuständigen Mitarbeitern des Ref. 5.2 vorgenommen werden.

(2) Der Betrieb von nicht dienstlich bereitgestellten Rechnern, Rechner-Bestandteilen und anderer IT-Technik ist grundsätzlich untersagt. Über Ausnahmen entscheidet das Ref. 5.2.

§ 3 Software

(1) Sämtliche Rechner werden grundsätzlich mit einem „Windows-basierten“ Betriebssystem ausgestattet. Dienstlich notwendige Ausnahmen davon sind mit Ref. 5.2 abzustimmen und werden durch Ref. 5.2 realisiert. Für die vernetzten Rechner wird derzeit "Novell-NetWare" als Netzwerkbetriebssystem eingesetzt.

(2) Aus Gründen des Datenschutzes, der Datensicherheit und zum Schutz vor unberechtigter Nutzung der Rechner und zum Zugang zum Datennetz der ZUV und des Rektorates wird auf jedem Rechner ein Zugangsclient zum Netzwerk installiert. Das entsprechende Passwort wird jeweils persönlich durch Ref. 5.2 zugewiesen.

(3) Zugelassen ist nur Software, die vom Ref. 5.2 beschafft oder ausdrücklich schriftlich zugelassen ist. Der Einsatz anderer, insbesondere privater, Software ist untersagt. Das Herunterladen von Software aus dem Internet und deren Installation ist untersagt, dies betrifft nicht automatische Updates, soweit diese vom Ref. 5.2 eingerichtet worden sind. Im Bedarfsfall wird Software über Ref. 5.2 geladen, verteilt und installiert. Ausnahmen von dieser Regelung sind nur in Ref. 5.2, und dann nur aus dienstlichen Erwägungen, gestattet.

(4) Die Originaldatenträger und die gefertigten Sicherungskopien der eingesetzten Software werden im Ref. 5.2 aufbewahrt. Das Ref. 5.2 führt über die zulässige Software ein Verzeichnis.

§ 4 Schulung, Literatur

(1) Jeder Nutzer wird vor der erstmaligen Aufnahme seiner Arbeit an einem Rechner oder vor der Installation neuer Programme im erforderlichen Umfang geschult. Für die Freistellung der jeweiligen Mitarbeiter für die Schulung und den Umfang der Schulungen ist die zuständige Abteilungsleitung verantwortlich.

(2) Den Nutzern wird die für die Bedienung der Geräte und Programme erforderliche Literatur (Bedienungsanleitungen, Handbücher) vom Ref. 5.2 zur Verfügung gestellt, sofern sie in schriftlicher Form vorliegt.

§ 5 Betrieb der Geräte

(1) Sollten nach dem Einschalten des Rechners während des Selbsttests bzw. bei der Arbeit am Rechner Fehlermeldungen auftreten, so darf die Arbeit am Rechner nicht aufgenommen oder fortgesetzt werden. Das Ref. 5.2 ist umgehend zu benachrichtigen.

(2) Nach Ablauf des Selbsttestes und der automatischen Konfiguration des Rechners erscheint auf dem Monitor der Anmeldedialog. Der Nutzer wird aufgefordert, sein vorher festgelegtes Passwort einzugeben und die Eingabe per Mausklick oder mit der "Enter-Taste" zu bestätigen.

Anschließend gelangt der Nutzer auf den Desktop, welcher die Nutzung der verschiedenen installierten Programme ermöglicht.

§ 6 **Passwort und Netzzugang**

(1) Für jeden Nutzer wird ein individuelles Passwort festgelegt, welches es ihm ermöglicht, in die für ihn freigegebenen Programme seines Rechners zu gelangen. Dieses Passwort wird in Ref. 5.2 nach geltenden Sicherheitsregeln generiert. Der Nutzer muss sich das Passwort in seiner genauen Schreibweise (Groß-/ Kleinbuchstaben) merken. Eine schriftliche Fixierung des Passwortes sollte möglichst unterbleiben, andernfalls aber so deponiert werden, dass Unbefugte nicht in den Besitz der Passwort-Notiz gelangen können. Der Nutzer trägt die Verantwortung dafür, dass das Passwort nicht an Dritte weiter gegeben wird. Falls der Verdacht besteht, dass ein Passwort Dritten bekannt geworden ist, ist dies Ref. 5.2 zu melden. Dem Nutzer wird dann schnellstmöglich durch Ref. 5.2 ein neues Passwort zugewiesen.

(2) Mit seinem Netzzugang wird dem Nutzer eine dienstliche E-Mail-Adresse durch Ref. 5.2 generiert. Eine eigenmächtige Veränderung an der E-Mail-Adresse und eine Veränderung der E-Mail-Konfiguration sind nicht zulässig. Änderungen (z. B. bei Namensveränderungen) sind Ref. 5.2 anzuzeigen und werden in Zusammenarbeit mit dem URZ geändert.

§ 7 **Datensicherung**

Für die zentral im Netz zur Verfügung gestellten Programme und die gespeicherten Nutzerdaten auf den Servern werden regelmäßige Sicherungen vom Ref. 5.2 vorgenommen. Für die Sicherung lokal am Rechner gespeicherter Daten sind die PC-Nutzer selbst verantwortlich. Gegebenenfalls benötigte Datenträger (z. B. Disketten, CD, DVD) sind im Ref. 5.2 zu erhalten.

§ 8 **Datensicherheit**

(1) Der Schutz der Daten vor Einsichtnahme und Veränderung durch Dritte wird durch das Passwortverfahren gewährleistet, sodass jedem Nutzer nur der Zugriff auf die Programme und Daten gestattet ist, für die er eine Berechtigung hat.

(2) Um die Betriebssicherheit des gesamten IT-Systems der ZUV und des Rektorates zu gewährleisten, können die Systembetreuer des Ref. 5.2 im Schadensfall (z. B. Virenbefall, Festplatten-Crash, u. a.) die lokal und zentral abgelegten Datenstrukturen der einzelnen Nutzer einsehen. Eine inhaltliche Kontrolle der Daten, etwa zum Zweck der Leistungskontrolle, findet nicht statt.

(3) Die Systembetreuer sind zur Verschwiegenheit verpflichtet.

(4) Die Verarbeitung personenbezogener Daten darf nur im Rahmen der dienstlichen Aufgaben erfolgen. Die Rechner, auf denen personenbezogene Daten verarbeitet werden, sind so aufzustellen, dass sie nicht von Besucherinnen oder Besuchern eingesehen werden können. Auf diesen Rechner ist außerdem ein Bildschirmschoner mit Passwortschutz so einzurichten, dass er sich bei Nichtbenutzung des Rechners automatisch einschaltet.

(5) Die Nutzung der IT-Komponenten für gewaltverherrlichende, pornografische und volksverhetzende Darstellungen in Bild, Ton oder Schrift ist untersagt. Ebenso sind Darstellungen untersagt, die Geschlecht, Rasse, Religion oder sexuelle Identität diskriminieren.

(6) Alle Räume mit Rechner-Arbeitsplätzen sind auch bei kurzfristiger Abwesenheit des bzw. der Bediensteten gegen den Zutritt Fremder zu sichern.

§ 9 Geheimhaltung

(1) Die Nutzer sind zur Geheimhaltung der ihnen anvertrauten Daten und Passwörter verpflichtet.

(2) Die Nutzer bestätigen entweder bei ihrer Einstellung oder nach Bekanntmachung/Veröffentlichung dieser Nutzungsregeln durch Unterschrift die Kenntnisnahme.

§ 10 Pflege der Geräte

(1) Die Rechner sind pfleglich zu behandeln. Wie alle elektronischen Geräte vertragen auch die einzelnen Rechner-Komponenten keine starken Erschütterungen, keine Feuchtigkeit und keine direkte Sonnen- und Wärmestrahlung. Vorhandene Belüftungsschlitze dürfen nicht verdeckt werden. Die an den einzelnen Geräten angeschlossenen Kabel dürfen nicht geknickt und nicht von den Geräten abgezogen werden. Auf den Rechnern und deren Bestandteilen dürfen keine Gegenstände abgestellt werden.

(2) Bildschirmoberflächen und Tastatur sollten regelmäßig mit vom Ref. 5.2 zu benennenden Reinigungsmitteln oder mit einem leicht mit Wasser angefeuchteten Papiertaschentuch gereinigt werden. Die Geräte sind vor der Reinigung auszuschalten.

(3) Nach Beendigung der Arbeit am Rechner ist das Gerät auszuschalten.

Diese Dienstanweisung tritt nach Unterzeichnung durch den Kanzler und am Tag nach ihrer Veröffentlichung im Amtsblatt in Kraft.

Halle (Saale), 23. September 2009

Dr. Martin Hecht
Kanzler