Regeln für die Nutzung der PC in der Verwaltung der Technischen Universität Clausthal

vom 10. November 1992
zuletzt geändert am 15.12.2011

Inhaltsübersicht

§ 1 - Zweck der Regeln

(1) Diese Regeln sollen den Nutzern der Personalcomputer (PC) in der Universitätsverwaltung als Hilfestellung und Richtschnur zum Umgang mit der DV-Technologie 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 des Dezernats 2 zur Hilfeleistung zur Verfügung.

(2) Diese Regeln erstrecken sich auf folgende Geräte und Gerätekomponenten der PC:

- die Zentraleinheit,
- die Tastatur,
- die Maus,
- der Monitor,
- der Drucker (soweit vorhanden)
- sonstige Peripheriegeräte (Scanner, etc.).

§ 2 - Hardware

(1) PCs werden nur vom Dezernat 2 beschafft und installiert. Änderungen an den PC sowie Eingriffe in die PC und deren Bestandteile dürfen nur von den zuständigen Mitarbeitern des Dezernats 2 vorgenommen werden.

(3) Der Betrieb von nicht dienstlich bereitgestellten PC oder PC-Bestandteilen ist grundsätzlich untersagt. Über Ausnahmen entscheidet das Dezernat 2 unter Anlegung strenger Maßstäbe.

§ 3 - Software

(1) Die Arbeitsplatz-PC werden mit den Betriebssystemen der Firma Microsoft betrieben (Windows XP/Win7), die den Zugang mittels Passwort zwingend erfordern.
Die Vernetzung erfolgt über TCP-IP. Der Intranetzugang der Nutzer an die Verwaltungsdomäne (Windows 2008 Server) wird über dieses Protokoll zugelassen. Weitere Protokolle werden nicht zugelassen. Der Zugang zum Internet ist nur über das Intranet zulässig.

(2) Zugelassen ist, außer der in den Netzen zentral zur Verfügung gestellten Software, nur Software, die vom Dezernat 2 beschafft oder ausdrücklich schriftlich zugelassen ist. Der Einsatz anderer Software ist nicht zulässig.

(3) Die Originaldatenträger und die gefertigten Sicherungskopien der eingesetzten Software werden im Dezernat 2 aufbewahrt. Das Dezernat 2 führt über die zulässige Software ein Verzeichnis.

§ 4 - Schulung, Literatur

(1) Jeder Nutzer wird vor der erstmaligen Aufnahme seiner Arbeit an einem PC oder vor der Installation neuer Programme im erforderlichen Umfang geschult.
(2) Den Nutzern wird die für die Bedienung der Geräte und Programme erforderliche Literatur (Bedienungsanleitungen, Handbücher) vom Dezernat 2 zur Verfügung gestellt.

§ 5 - Betrieb der Geräte

(1) Bei während des Betriebs auftretenden Fehlermeldungen sollte die Arbeit am PC nicht aufgenommen oder fortgesetzt werden. Das Dezernat 2 ist umgehend zu benachrichtigen.

(2) Das Gerät durchläuft nach dem Einschalten einen Selbsttest und die automatische Konfiguration des PC erscheint auf dem Eingangsbildschirm. Der Nutzer wird aufgefordert, sein vorher festgelegtes Passwort einzugeben und die Eingabe mit der "Enter-Taste" zu bestätigen. Anschließend gelangt der Nutzer auf einen Desktop, welcher - auf die individuellen Erfordernisse des Arbeitsplatzes zugeschnitten - die Nutzung der verschiedenen Programme und typischen Arbeitsschritte ermöglicht.

(3) Nutzdaten sollten nicht unter dem Profil des jeweiligen Nutzers gespeichert werden, sondern sind aus Datensicherungsgründen auf dem Server zu speichern. Private Daten der Nutzer dürfen nicht auf dem Server abgespeichert werden; solche können im Bedarfsfall lokal gespeichert werden. Zweifelsfälle klärt das Dezernat 2.

§ 6 - Passwort

(1) Für jeden Nutzer wird ein individuelles Passwort festgelegt, welches ihm ermöglicht, in die für ihn freigegebenen Programme seines PC und auf die zugelassenen Datenbereiche auf dem Server zu gelangen. Der Nutzer muss sich das Passwort in seiner genauen Schreibweise (Groß-/Kleinbuchstaben) merken.
Eine schriftliche Fixierung des Passwortes sollte unterbleiben. Falls dies nicht möglich ist, sollte das Passwort so deponiert werden, dass Unbefugte nicht in den Besitz der Passwort-Notiz gelangen können (ein unter die Tastatur gelegter oder geklebter Notizzettel erfüllt beispielsweise nicht die Sicherheits-Anforderungen). Die Nutzer werden in regelmäßigen Abständen (30 Tage) vom System aufgefordert, das Passwort zu wechseln.

(2) Die Länge des Passwortes muss mindestens 6 Zeichen betragen und sollte möglichst kein Leerzeichen enthalten. Die letzten 6 Passworte können nicht wiederholt werden und sollten nicht ähnlich lauten.

(3) Besondere Anforderungen sind an die Passwörter im Bereich der Kidicap-Software zu stellen. Hier muss die Länge der Passwörter 7 Zeichen betragen. Die Passwörter müssen dabei mindestens einen Großbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

§ 7 - Datensicherung

(1) Von jedem Nutzer sollen regelmäßig Datensicherungen seiner lokal gespeicherten Daten durchgeführt werden. In der Praxis hat sich das Verfahren bewährt, von den jeweiligen Datenbeständen mindestens 2 Sicherungskopien anzulegen (sog. Vater-Sohn-Prinzip).
In regelmäßigen Abständen sollte eine Datensicherung auf dem Server vorgenommen werden. Ferner werden für die Datensicherung benötigten Datenträger vom Dezernat 2 zur Verfügung gestellt

(2) Bei den zentral in den Netzen zur Verfügung gestellten Programmen und Daten (SOS, POS, SAP R/3) werden regelmäßige Sicherungen vom Dezernat 2 vorgenommen. Die für jeden Nutzer angelegten Profile und privaten Netzwerkordner werden täglich gesichert.

§ 8 - Datensicherheit

(1) Der Schutz der Daten vor Einsichtnahme und Veränderung durch Dritte wird durch das Passwortverfahren gewährleistet, so dass jedem Nutzer nur der Zugriff auf die Programme und Daten gestattet ist, für die er eine Berechtigung hat. Bei Daten mit höherer Schutzstufe (z.B. SAP/HR) werden die Daten verfahrensbezogen verschlüsselt übertragen.
Ferner können für die lokale Speicherung personenbezogener Daten sog. Datensafes installiert werden, die den Zugriff betriebssystemunabhängig regeln.

(2) Nur die Systembetreuer des Dezernats 2 haben die Möglichkeit, sämtliche Daten, die auf den einzelnen PC und den zentralen Speichersystemen abgelegt sind, einzusehen. Einzige Ausnahme bilden die o. g. lokalen Datensafes. Diese umfangreichen Zugriffsrechte sind aufgrund der Aufgabenstellung der Systembetreuer notwendig. Die Einsichtnahme in die Datenstrukturen der einzelnen Nutzer erfolgt nur, um die Betriebssicherheit des Systems zu überprüfen bzw. herzustellen.
Eine inhaltliche Kontrolle der Daten, etwa zum Zweck der Leistungskontrolle, findet nicht statt.

(3) Die Systembetreuer sind zur Verschwiegenheit verpflichtet.

(4) Die PC, auf denen personenbezogene Daten verarbeitet werden, sind so aufzustellen, dass sie nicht von Besucherinnen oder Besuchern eingesehen werden können. Diese PC sind außerdem mit einem Bildschirmschoner ausgestattet, der bei Nichtbenutzung des PC den Bildschirm automatisch oder manuell dunkel schaltet. Der Bildschirm ist dann nur mit Passwort wieder zu aktivieren.

(5) Alle Räume mit Arbeitsplatz-PC sind auch bei kurzfristiger Abwesenheit des Bediensteten abzuschließen.

§ 8a - Geheimhaltung

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

§ 9 - Pflege der Geräte

(1) Die PC sind pfleglich zu behandeln. Wie alle elektronischen Geräte vertragen auch die einzelnen PC-Bestandteile 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. Die Einnahme von Getränken und Speisen sowie das Rauchen im unmittelbaren Bereich der Tastatur ist nicht zulässig. Auf den PC und deren Bestandteilen dürfen keine Gegenstände abgestellt werden.

(2) Das Reinigen der Bildschirmoberfläche (LCD/TFT) sollte möglichst nur mit einem fuselfreien, weichen Tuch äußerst vorsichtig erfolgen, da diese sehr empfindlich ist. Ist das Monitorgehäuse stark verschmutzt ist es hier ratsam nur mit einem feuchten Tuch zu säubern. Es sollte nur warmes Wasser (keine Lösungs- oder sonstige Säuberungsmittel) genommen werden, nachtrocknen ebenfalls mit einen trockenen Tuch. Scharfe Reinigungsmittel können die gesamte Oberfläche angreifen.

(3) Aus Gründen des Daten- und Geräteschutzes sollte bei Gewittern die Arbeit an den PC eingestellt werden und die Netzstecker aus den Steckdosen gezogen werden.

(4) Bei Beendigung der Arbeit am PC ist das Gerät und seine Komponenten (Bildschirm, Drucker etc.) auszuschalten. Begründete Ausnahmen sind mit dem Dezernat 2 abzustimmen und schriftlich festzuhalten. Soweit vorhanden ist der PC elektrisch, durch schalten an der Steckerleiste oder Hauptschalter, von der elektrischen Versorgung zu trennen. Bei längerer Abwesenheit des Benutzers während des Dienstes ist der PC zur Energieeinsparung ebenso auszuschalten.

§ 10 - Kenntnisnahme

(1) Die Mitarbeiter und Mitarbeiterinnen bestätigen bei ihrer Einstellung durch Unterschrift die Kenntnisnahme dieser PC-Anweisung.