Regeln für den Einsatz von DV-Geräten im Verwaltungsnetz (Stand Mai 2011)

1. Regeln für die Verwendung von Passwörtern

Die Gestaltung des Passworts

Bei der Auswahl eines Passwortes muß darauf geachtet werden, daß es nicht leicht ermittelbar ist. Zum Ermitteln von Passwörtern durch Unbefugte werden heutzutage automatische große Wortlisten abgeprüft. Die darin enthaltenen Wörter stammen aus diversen Wörterbüchern, Namenssammlungen usw.. Deshalb müssen unbedingt einige Gestaltungshinweise beachtet werden, wenn die Passworte ihre Funktion, Unbefugte vom Zugriff aufgeschützte Daten fernzuhalten, erfüllen sollen:

- Das Passwort darf auf keinen Fall leicht erratbar sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden
- Innerhalb des Passwortes sollte mindestens ein Zeichen verwendet werden, das kein Buchstabe ist (Sonderzeichen oder Zahl)
- Ein neu vergebenes Passwort muß sich vom bisher verwendeten Passwort unterscheiden
- Es sollte mindestens 8 Zeichen lang sein

Der Umgang mit Passwörtern

- Voreingestellte Passwörter, z.B. bei der Auslieferung eines PCs, müssen durch individuelle Passwörter ersetzt werden
- Passwörter dürfen nicht auf programmierbare Funktionstasten gespeichert werden
- Das Passwort muß regelmäßig gewechselt werden
- Das Passwort muß geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein. Auf keinen Fall sollte das Passwort innerhalb einer Datei auf dem PC oder auf einem frei zugänglichen Zettel hinterlegt sein. Das Passwort sollte allenfalls für den Vertretungsfall schriftlich fixiert werden, wobei es in diesem Fall in einem verschlossenen Umschlag sicher aufbewahrt werden muß.
- Das Passwort muß geändert werden, wenn das Passwort unautorisierten Personen bekannt geworden ist
- Vergessenes Passwort: Hat ein Nutzer sein individuelles Passwort vergessen, dann wird dieses auf Veranlassung des Nutzers von den zuständigen Mitarbeiter/innen der Verwaltungs-EDV durch ein neues ersetzt
- Passwörter dürfen nicht abgespeichert werden, auch wenn dies von der verwendeten Software (z.B. Outlook, Eudora) angeboten wird

2. Regeln für den Einsatz von Soft- und Hardware

Nutzungsverbot nicht freigegebener Programme

An den DV-Arbeitsplätzen im Verwaltungsnetz dürfen ausnahmslos nur freigegebene Programme eingesetzt werden. Zuständig sowohl für die Freigabe eines Programms als auch für dessen Installation sind ausschließlich die Mitarbeiter/innen des Sachgebiets „Administrative EDV-Systeme und Support“. Grundsätzlich werden nur Programme freigegeben, an deren Nutzung ein dienstliches Interesse besteht. Es ist zu beachten, daß sich jeder schadensersatzpflichtig macht, der ein nicht freigegebenes Programm selbst einspielt, das dann Anlass für einen Schaden ist. Ferner macht sich jeder strafbar, der bewusst lizenzpflichtige Programme einsetzt, für die keine Lizenz erworben wurde.

Kopierverbot dienstlicher Software
Dienstliche Software darf nicht, außer in Absprache mit den Mitarbeite/innen des Sachgebiets „Administrative EDV-Systeme und Support“, kopiert werden.

Einspielverbot privater Daten, Verwendung von Bildschirmschonern
Auf den DV-Arbeitsplätzen und auf den Netzlaufwerken dürfen keine privaten Daten eingespielt werden. Bildschirmschoner, bei denen es sich nicht um die standardmäßig von Windows angebotenen handelt, dürfen nur nach Rücksprache mit den Mitarbeitern des Sachgebiets „Administrative EDV-Systeme und Support“ verwendet werden

Manipulationsverbot an dienstlicher Hardware
Es ist nicht erlaubt, an dienstlich zur Verfügung gestellter Hardware selbstständig Manipulationen vorzunehmen. So dürfen durch die Nutzer z.B. weder neue Komponenten eingebaut noch alte Komponenten ausgetauscht werden.

Nutzungsverbot privater Hardware
Private Hardware wie z.B. PDAs, externe USB-Speichermedien dürfen nicht an den DV-Arbeitsplätzen im Verwaltungsnetz eingesetzt werden.

3. Regeln für den Betrieb des PCs

- Bildschirme und Drucker sind so aufzustellen bzw. abzuschirmen, dass weder der Bildschirminhalt noch die Druckausgabe von Unbefugten eingesehen werden kann. Wichtig ist dies v.a. in Arbeitsräumen mit Publikumsverkehr.
- Wenn Sie Ihren Arbeitsraum verlassen, sollten Sie das Büro abschließen. Sollte dies nicht möglich sein, so sollten Sie den Bildschirm sperren. Dazu drücken Sie STRG+ALT+Entf, und wählen auf dem dann angezeigten Bildschirm „Arbeitsstation sperren“ aus. Entsperrt wird die Arbeitsstation durch die Eingabe Ihres Novell-Passworts.

4. Regelungen für das Verhalten bei sicherheitsrelevaten Ereignissen und bei sonstigen Hardware- und Softwarestörungen

Alle sicherheitsrelevanten Ereignisse (z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht

explizit freigegebener Dienste, Verdacht auf Mißbrauch der eigenen Benutzerkennung, Auftreten eines Computer-Virus usw.) sowie sonstige Hard- und Softwarestörungen sind sofort an das Sachgebiet „Administrative EDV-Systeme und Support“ zu melden. Dort wird der Angelegenheit nachgegangen bzw. werden weitere Schritte veranlasst.

5. Regeln für die Behandlung von Festplatten, Disketten, CDROMs, DVDs, USB-Sticks und anderen Speichermedien

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.

Löschung bzw. Vernichtung
Datenträger müssen bevor sie entsorgt bzw. an Dritte weitergegeben werden, zuverlässig gelöscht werden. Dafür müssen diese Datenträger an das Sachgebiet „Administrative EDV-Systeme und Support“ übergeben werden.

6. Aussonderung gebrauchter Geräte

DV-Geräte, die nicht mehr gebraucht werden, müssen den Mitarbeiter/innen des Sachgebiets „Administrative EDV-Systeme und Support“ gemeldet werden. Diese sorgen dann für eine fachgerechte Wiederverwendung bzw. Entsorgung der Geräte.

7. Regeln für den Einsatz von E-Mail

- Für den Inhalt einer Email ist der jeweilige Absender verantwortlich
- E-Mails sollten keine Inhalte enthalten, die Sie nicht auch in Papierform veröffentlichen würden
- Die offene, ungeschützte Übertragung von sensiblen, schutzwürdigen und insbesondere personenbezogenen Daten via Email ist nicht zulässig. Entweder müssen diese Daten verschlüsselt werden oder der Zugriff auf die Daten muss durch ein Kennwort geschützt werden. Das Kennwort müssen Sie dann dem Empfänger mitteilen. In Word funktioniert der Kennwortschutz z.B. wie folgt:
  Klicken Sie im Menü **Datei** auf **Speichern unter**. Klicken Sie im Dialogfeld **Speichern unter** im Untermenü **Extras** auf **Allgemeine Optionen**. Geben Sie im Feld **Kennwort für Lese-/Schreibzugriff** ein Kennwort ein, und klicken Sie dann auf **OK**. Geben Sie im Feld **Kennwort erneut eingeben** das Kennwort erneut ein, und klicken Sie auf **OK**. Klicken Sie auf **Speichern**.
- Lassen Sie sich den Erhalt von wichtigen Emails vom Empfänger durch eine Email oder durch einen Anruf bestätigen
- Ausführbare Programme und ausführbare Programmcodes dürfen nur in begründeten Einzelfällen per Email verschickt werden. Werden derartige

Dateien empfangen, so dürfen die betroffenen Mitarbeiter/innen diese nicht ausführen (Achtung: Virengefahr). Eine Ausnahme besteht dann, wenn die Datei von vertrauenswürdiger Stelle angekündigt wurde. Besonders kritisch sind alle ausführbaren Programme (wie .COM, .EXE, .PIF) oder Skript-Sprachen (.VBS, .JS, .BAT), Registrierungsdateien (.REG) sowie Bildschirmschoner (.SCR).

- Eine eingehende Email ist mit der üblichen Sorgfaltspflicht in den Geschäftsgang zu geben. Sie kann dazu entweder ausgedruckt oder weitergeleitet werden.
- Das Ändern von Einstellungen des E-Mail-Programms ist nur in begründeten Einzelfällen erlaubt
- Rufen Sie Ihre Emails mindestens einmal am Tag ab
- Füllen Sie die Betreffangaben (Subject) immer aus, entsprechend der Betreffangaben in einem Anschreiben
- Verwenden Sie beim Verfassen einer Email möglichst keine Sonderzeichen, Umlaute und Formatierungen. Dies gilt v.a. bei Emails, die aus dem Verwaltungsnetz hinaus gehen und bei denen das verwendete Email-Programm unbekannt ist
- Wählen Sie für das Abrufen Ihrer Emails ein geeignetes Passwort (s. 1. Regeln für die Verwendung von Passwörtern). Speichern Sie Ihr Passwort auf keinen Fall dauerhaft im Email-Programm ab. Dies stellt ein großes Sicherheitsrisiko dar.
- Die Weiterleitung oder Ablage von (dienstlichen) E-Mails auf einen Mail-Server außerhalb der Universität z.B. web.de oder googlemail ist generell untersagt.

8. Regeln für den Einsatz von WWW

- Es dürfen, mit Ausnahme von begründeten Einzelfällen, keine Programme oder ausführbare Programmcodes aus dem Internet heruntergeladen werden
- Geben Sie in keinem Fall Ihre persönlichen und beruflichen Daten im Internet in Formularfeldern oder dergleichen weiter, außer dies ist für die Erfüllung Ihrer dienstlichen Aufgaben erforderlich (z.B. online-Kreditkarten-Bestellungen durch die Beschaffung)
- Lassen Sie sich nicht mit WWW-Seiten verbinden, deren Adressen nicht mit „http:“ oder „https:“ beginnen.
- Verändern Sie in keinem Fall die vorgegebenen Einstellungen Ihres WWW-Browsers
- Der Zugriff und die Nutzung von Tauschbörsen ist verboten
- Unzulässig ist jede Internetnutzung, die geeignet erscheint, den Interessen der Universität Konstanz oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze oder Verordnungen verstößt

9. Laptops im Verwaltungsnetz

Laptops dürfen im Verwaltungsnetz nur dann benutzt werden, falls sie dort ausschließlich verwendet werden. Eine wechselnde Benutzung im öffentlichen

Netz (W-Lan) und im Verwaltungsnetz ist aus sicherheitstechnischen Gründen nicht gestattet.

10. Speichern wichtiger Dateien

Speichern Sie generell alle dienstlich wichtigen Dateien auf den entsprechenden Netzlaufwerken (z.B. Laufwerk p (persönlich) oder Laufwerk o (Abteilungslaufwerk). Diese werden dann durch ein Backupsystem jede Nacht vollständig gesichert.

11. Der aufgeräumte Arbeitsplatz

Sie sollten Ihren Arbeitsplatz „aufgeräumt“ hinterlassen. Das heißt, dass dafür Sorge zu tragen ist, dass Unbefugte keinen Zugang zu IT-Anwendungen oder Daten erhalten. Es darf außerdem nicht möglich sein, dass Unbefugte auf Datenträger oder Unterlagen zugreifen können.

Bei kurzer Abwesenheit während der Arbeitszeit sollten Sie den Raum, sofern möglich, verschließen und/oder den Bildschirm sperren, so dass Zugriffe nur nach erfolgreicher Anmeldung möglich sind. Bei längerer Abwesenheit (Besprechungen, Dienstreisen, Urlaub) sollten Sie Ihren Arbeitsplatz so aufräumen, dass keine schutzbedürftigen Datenträger oder Unterlagen unverschlossen am Arbeitsplatz zurückgelassen werden.