UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

backUP

MAGAZIN FÜR IT-SICHERHEIT

backUp Magazin für IT-Sicherheit
04 / 2003
Ausgabe
Nr. 04
2003

PC-ARBEITSPLATZ

Soviel Datenschutz muss an jedem Arbeitsplatz sein!

HERAUSGEBER: Unabhängiges Landeszentrum
für Datenschutz Schleswig-Holstein
Postfach 71 21 | 24171 Kiel
Ansprechpartner: Heiko Behrendt
Telefon: (0431) 988 - 12 12 | Telefax: (0431) 988 - 12 23
E-Mail: mail@datenschutzzentrum.de
Homepage: www.datenschutzzentrum.de

TITEL-DESIGN: Eyekey Design, Kiel
www.eyekey.de

DRUCK: Druckerei A.C. Ehlers, Kiel

AUFLAGE: 1. Auflage, Juni 2003

Vorwort

Liebe Leserinnen, liebe Leser!

Datenschutz ist in aller Munde und doch für viele ein Buch mit sieben Siegeln. Dabei geht es im Kern um ein paar leicht verständliche und in der Praxis auch gut umsetzbare Prinzipien. Auch wenn es in erster Linie Sache der Behörden- oder Firmenleitung ist, den Datenschutz richtig zu organisieren, so ist doch auch jeder einzelne gefordert, seinen Beitrag zu leisten.

In diesem ***backUP-Magazin*** geht es um die wichtigsten Datenschutzgrundsätze, die an jedem Arbeitsplatz berücksichtigt werden sollten – übrigens nicht nur im Interesse der Kunden und Bürger, sondern auch im eigenen Interesse der Mitarbeiter. Denn klare Verhältnisse am PC-Arbeitsplatz entlasten im Zweifel auch die Mitarbeiterinnen und Mitarbeiter, wenn es zu Pannen kommt.

backUP-Magazine wollen praktische Tipps für den Datenschutz am PC-Arbeitsplatz geben, die jeder gut umsetzen kann. Sollten noch Fragen offen sein, so stehen das Unabhängige Landeszentrum für Datenschutz und die im Impressum genannten Autoren und Ansprechpartner gerne für weitergehende Informationen zur Verfügung.

backUP-Magazine erscheinen in unregelmäßigen Abständen und werden unentgeltlich zur Verfügung gestellt. Sie sind Teil unserer Konzeption des *neuen* Datenschutzes, der neben der Kontrolltätigkeit vor allem auf Beratung und Service setzt.

Die Dynamik der hard- und softwaretechnischen Veränderungen im Bereich der automatisierten Datenverarbeitung bringt es mit sich, dass ***backUP-Magazine*** laufend aktualisiert werden müssen. Für diesbezügliche Anregungen sowie für generelle Verbesserungsvorschläge sind wir dankbar.

Kiel, im Mai 2003

Dr. Helmut Bäumler

Landesbeauftragter für den Datenschutz

INHALT

Haben Sie auf alle Fragen eine Antwort?

Was ist Datenschutz?

Was muss ich bei meiner Arbeit mit dem Computer beachten?

An welche Datenschutzgesetze muss ich mich halten?

Ist Datensicherheit das Gleiche wie Datenschutz?

Was ist bei Computern anders als bei Akten?

Wie vernichte ich Papier/Unterlagen mit personenbezogenen Daten?

Gibt es für meinen Arbeitsbereich spezielle Richtlinien zum Umgang mit Daten?

Wer kann auf meinem Computer arbeiten?

Wo werden „meine“ Daten gespeichert?

Kann jemand überwachen, was ich auf meinem Computer mache?

Warum können das Disketten- und das CD-ROM-Laufwerk ein Sicherheitsrisiko sein?

Wie organisiere ich meine Datenablage?

Warum brauche ich ein Passwort?

Was muss ich beim Umgang mit dem Passwort beachten?

Welche Sicherheitsprobleme können sich bei Microsoft-Office-Produkten ergeben?

Wie gewährleiste ich den Datenschutz beim Publikumsverkehr?

Wann ist eine Verschlüsselung sinnvoll?

Was muss ich bei der E-Mail-Kommunikation beachten?

Wie gefährlich ist das Internet?

Wenn ja, sollten Sie diese mit den nachfolgenden Hinweisen abgleichen,

wenn nein, können Sie Ihre Wissenslücken schließen, indem Sie sich die nachfolgenden Hinweise sorgfältig ansehen.

Hinweis

Die praktische Umsetzung der Datenschutzmaßnahmen am PC-Arbeitsplatz werden in diesem ***backUP-Magazin*** am Beispiel des Betriebssystems **Microsoft Windows XP** dargestellt. Grundsätzlich sind diese Maßnahmen aber auf jedes andere Betriebssystem übertragbar.

1. Grundlagen

In diesem Kapitel soll kurz auf die häufigsten und wichtigsten Fragen in Bezug auf den Datenschutz eingegangen werden.

Sie möchten noch mehr wissen? Dann können Sie als Mitarbeiter öffentlicher Stellen auf das Landesdatenschutzgesetz und die Datenschutzverordnung und als Mitarbeiter im nichtöffentlichen Bereich auf das Bundesdatenschutzgesetz zurückgreifen.

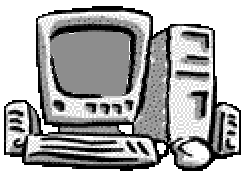
Was sind personenbezogene Daten?

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, z. B. der Name und die Anschrift (bestimmte Person) bzw. das Autokennzeichen oder die Ausweisnummer (bestimmbare Person).

Was versteht man unter Datenverarbeitung?

Datenverarbeitung umfasst das Erheben, Speichern, Übermitteln, Sperren, Löschen, Anonymisieren und Verschlüsseln von Sachinformationen oder personenbezogenen Informationen (Daten).

Was ist automatisierte Datenverarbeitung?



Die automatisierte Datenverarbeitung unterstützt die Arbeitsabläufe mithilfe von informationstechnischen Geräten (Hardware), Programmen (Software) und automatisierten Dateien (Daten).

Was ist Datenschutz?

Datenschutz ist der Schutz des Bürgers vor dem Missbrauch seiner Daten und gleichzeitig das Recht des Bürgers, selbst über die Preisgabe seiner Daten zu entscheiden.

Was ist Datensicherheit?

Datensicherheit umfasst alle technischen und organisatorischen Maßnahmen, um bewusste oder fahrlässige unzulässige Aktivitäten wie z. B.

- unbefugte Kenntnisnahme von Daten,
- unbefugte Löschung von Programmen oder
- eine Verfälschung von Daten

abzuwehren.

Welche Grundsätze der Datensicherheit sollten Sie beachten?

Verarbeiten Sie Daten automatisiert, dann sollten Sie deren Vertraulichkeit, Integrität und Verfügbarkeit sicherstellen.

Vertraulichkeit bedeutet, dass nur diejenigen Personen Zugriff auf die Daten erhalten, die auch das entsprechende Recht dazu besitzen.

Das lässt sich bei der papierenen Datenverarbeitung mit einem Aktenschrank vergleichen, für den nur die Mitarbeiter einen Schlüssel besitzen, die auch die Akten bearbeiten dürfen. Im Bereich der automatisierten Datenverarbeitung werden dagegen den Mitarbeitern über Benutzerkonten Zugriffsberechtigungen zugewiesen (näheres in Kapitel 6).

Integrität bedeutet, dass Daten vor Manipulationen geschützt werden. Aber auch fehlerhafte Software oder technische Störungen dürfen keine Veränderungen in den Datenbeständen hervorrufen.

Dieser Grundsatz wird in der papierenen Datenverarbeitung durch den Verschluss vertraulicher Unterlagen sichergestellt. Bei der automatisierten Datenverarbeitung hat die Gewährleistung der Integrität noch größere Bedeutung, da das Risiko des Manipulierens von Daten in automatisierten Fachverfahren relativ groß ist (näheres im Kapitel 10).

Verfügbarkeit gewährleistet, dass die Daten nicht verloren gehen und stets abrufbarbereit sind. In der papierenen Datenverarbeitung wird die Verfügbarkeit dadurch sichergestellt, dass z. B. immer ein Schlüssel für den Aktenschrank mit den Datenbeständen vorhanden ist. In der

automatisierten Datenverarbeitung muss sichergestellt sein, dass der Zugriff auf die Daten durch den Ausfall von IT-Systemen nicht beeinträchtigt wird.

Welche Verantwortung tragen Sie bei der Nutzung automatisierter Verfahren in Bezug auf den Datenschutz?

- Sie müssen bei der Verarbeitung personenbezogener Daten in Ihrem Aufgabenbereich die geltenden Datenschutzbestimmungen einhalten.
- Sie sind für die Einhaltung der Regelungen, die für Ihren Arbeitsplatz gelten, verantwortlich.
- Sie sind selbst für die ordnungsgemäße Nutzung der Ihnen zur Verfügung gestellten Hard- und Software zuständig.

Worauf müssen Sie bei der Verarbeitung personenbezogener Daten besonders achten?

(1) Die Verarbeitung von personenbezogenen Daten ist nur zulässig, wenn

- die schriftliche Einwilligung des Betroffenen vorliegt oder
- eine gesetzliche Befugnisregelung sie gestattet.

Das gilt für alle Formen der Datenverarbeitung, insbesondere für das

- Erheben,
- Speichern
- Übermitteln und
- Löschen von Daten.

(2) Die gesetzliche Befugnisregelung finden Sie in den jeweiligen Spezialgesetzen (z. B. Sozialgesetzbücher, Landesverwaltungsgesetz, Abgabenordnung sowie im Landesdatenschutzgesetz selbst). Wenn eine gesetzliche Befugnisgrundlage die geplante Datenverarbeitung gestattet, kommt es auf die Einwilligung des Betroffenen nicht an.

(3) Bei **Datenübermittlungen** an andere Stellen sollten Sie prüfen, ob die Daten für die Aufgabenerfüllung des Empfängers erforderlich sind und der ursprüngliche Verarbeitungs-

zweck beibehalten wird bzw. ob eine zweckändernde Nutzung durch den Empfänger erlaubt ist. Das gilt auch für Datenweitergaben **innerhalb** der Verwaltung!

(4) Über personenbezogene Daten dürfen Sie nur **Auskünfte** erteilen, wenn Sie sich außerdem in Bezug auf die Identität des Auskunftsersuchenden sicher sind. Bevollmächtigten dürfen Sie nur nach Vorlage einer schriftlichen Vollmacht Auskunft erteilen.

(5) **Löschen** Sie personenbezogene Daten, wenn ihre Speicherung unzulässig war oder ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist.

(6) Die Betroffenen haben das Recht, kostenlos **Auskunft** über die zu ihrer Person gespeicherten Daten zu verlangen.

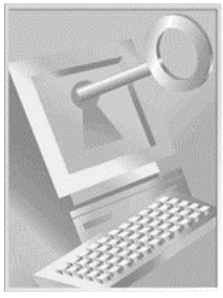
2. *Allgemeine Regeln*

Die Gewährleistung des Datenschutzes und der Datensicherheit am Arbeitsplatz erfordert genaue Vorgaben darüber, was zulässig und wie im Einzelfall zu verfahren ist. Diese Vorgaben sollten speziell auf die Benutzerarbeitsplätze zugeschnitten werden.

Die Leitungsebene fasst diese Vorgaben in einem **Sicherheitskonzept** zusammen und formuliert für die Mitarbeiter eine **Dienstanweisung**, die alle Fragen zu Datenschutz und Datensicherheit am Arbeitsplatz, den richtigen Umgang mit Daten, Datenträgern und Listen, Auskunftsfragen und Vorschriften zur Autorisierung von Anwendungen beinhalten sollte (Musterdienstanweisungen finden Sie im Anhang). Zu den wesentlichen Aufgaben der Leitungsebene gehört deshalb auch die **Unterweisung** bzw. die **Schulung** der Mitarbeiter in Bezug auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.

Auf der Administrationsebene werden diese Richtlinien technisch umgesetzt. **Doch Datenschutz und Datensicherheit enden nicht beim Administrator!** Auch jeder Mitarbeiter kann an einem PC-Arbeitsplatz die Risiken der personenbezogenen Datenverarbeitung minimieren, indem er allgemeine technische und organisatorische Regeln beachtet.

Die nachfolgende Auflistung gibt einen Überblick über die allgemeinen Regeln für den PC-Arbeitsplatz. Einige Regeln werden in den nachfolgenden Kapiteln aufgegriffen und vertieft. Im Anhang finden sich ausführliche Checklisten zu den behandelten Themen.



Allgemeine Regeln für den PC-Arbeitsplatz:

Sie sollten als Mitarbeiter

- *beim Verlassen Ihres Büros entweder die Tür verschließen oder den PC sperren (Strg + Alt + Entf und SPERREN),*
- *Ihre Schlüssel zum Büro, Schreibtisch usw. sicher verwahren,*
- *Ihre Unterlagen mit personenbezogenem Inhalt bei Abwesenheit unter Verschluss halten (Schrank, Schreibtisch),*

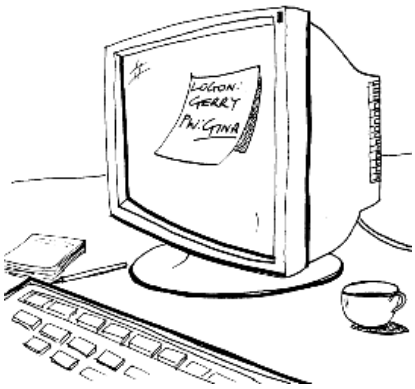
- *sicherstellen, dass sich Besucher nur in Ihrem oder im Beisein eines anderen Mitarbeiters im Büro aufhalten; achten Sie darauf, dass die Besucher keine "fremden" personenbezogenen Daten zur Kenntnis nehmen können,*

- *keine fehlgeschlagenen Kopien mit personenbezogenem Inhalt in den Papierkorb neben dem Kopierer werfen,*
- *dafür sorgen, dass die in Ihrem Papierkorb gesammelten personenbezogenen Unterlagen unter Aufsicht geschreddert werden,*
- *Unterlagen mit personenbezogenen Daten vernichten (am besten: Schredder!), wenn sie nicht mehr erforderlich sind; beachten Sie die bereichsspezifischen Aufbewahrungsfristen,*
- *keinem Unbefugten Zugriff auf Ihren Arbeitsplatz-PC und Ihre Fachanwendungen gewähren,*
- *darauf achten, dass der Bildschirm so ausgerichtet ist, dass kein Unbefugter/Besucher die Daten auf dem Bildschirm lesen kann,*
- *keinem Ihrer Kollegen die Möglichkeit geben, unter Ihrem Anmeldenamen und Passwort zu arbeiten,*
- *einen passwortgeschützten Bildschirmschoner einsetzen,*
- *Ihr Passwort sorgfältig auswählen, geheim halten und nicht aufschreiben,*
- *nur die personenbezogenen Daten verarbeiten, die Sie für Ihr Aufgabengebiet benötigen,*
- *regelmäßig prüfen, welche Daten Sie nicht mehr benötigen und diese dann löschen,*
- *keine personenbezogenen Daten auf der Festplatte Ihres PC speichern,*
- *Datenträger (Disketten, CD-ROMs) verschlossen aufbewahren,*
- *"alte" oder defekte Datenträger (Disketten, CD-ROMs) nicht einfach wegwerfen, sondern sie beim Administrator zur zentralen Vernichtung abgeben,*
- *die Standardsoftware nicht dazu benutzen, Eigenentwicklungen ohne Genehmigung zu programmieren,*
- *keine private Software oder private Datenträger mitbringen,*
- *keine Veränderungen an der Hardware Ihres PC vornehmen,*

- *personenbezogene Daten außerhalb der Räumlichkeiten Ihrer Behörde/Stelle nur auf dienstlichen mobilen PC zu dienstlichen Zwecken verarbeiten,*
- *nur mobile PC benutzen, deren Festplatten verschlüsselt sind,*
- *E-Mails mit personenbezogenen Daten nur in verschlüsselter Form versenden und*
- *empfangene E-Mails nach Bearbeitung bzw. Ausdruck löschen.*

Sofern es in Ihrer Organisation keine Richtlinien bzw. Dienstanweisungen gibt, die den Umgang mit personenbezogenen Daten in der papierenen und automatisierten Datenverarbeitung regeln, sollten Sie den Datenschutzbeauftragten oder Ihren Fachvorgesetzten ansprechen.

3. *Passwortschutz*



Möchten Sie an Ihrem Arbeitsplatz-PC arbeiten, werden Sie nach dem Einschalten des PC aufgefordert, Ihren Benutzernamen und das Passwort einzugeben. Das setzt voraus, dass der Administrator für Sie ein Benutzerkonto angelegt hat. Melden Sie sich das erste Mal am System an, so müssen Sie das vom Administrator vorgegebene Passwort ändern. Das hat den Vorteil, dass nur Sie Ihr Passwort kennen. Diese Angaben werden bei allen weiteren Anmeldungen vom System daraufhin überprüft, ob Sie das Recht besitzen, an diesem PC zu arbeiten. Stimmen die Angaben überein, können Sie auf die Systemfunktionen und Anwendungen Ihres Arbeitsplatzes zugreifen. Stimmen die Angaben hingegen nicht überein, wird Ihnen der Zugriff verwehrt und Sie werden erneut zur Eingabe des Passwortes aufgefordert. Das Passwort bildet sozusagen den Schlüssel zum System, mit dem Sie besonders verantwortungsvoll umgehen müssen.

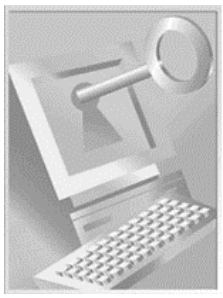
Die Administratoren tragen für die Bildung und Verwendung des individuellen Passwortes keine Verantwortung, sie haben "nur" die Möglichkeit, Richtlinien für die Verwendung von Passwörtern zu aktivieren. Folgende Einstellungen stehen den Administratoren zur Verfügung:

- *Kennwortvergabe:* Die Benutzer müssen bei Neueinrichtung ihres Benutzerkontos oder nach der Rücksetzung eines vergessenen Passwortes ein vom Administrator zugeteiltes Passwort bei der ersten Anmeldung ändern.
- *Mindestlänge:* Ein Zugang ohne Passwort und mit einem, das weniger als 6 Zeichen umfasst, ist nicht möglich.
- *Kennwortalter:* Spätestens nach drei Monaten wird zur Änderung des Passwortes aufgefordert.
- *Kennwortchronik:* Verwendete Passwörter dürfen nach einer Änderung nicht wieder benutzt werden.
- *Kontosperrung:* Nach mehrmaliger Falscheingabe des Passwortes wird das Benutzerkonto auf Dauer gesperrt. Nur der Administrator kann die Sperrung aufheben.
- *Überwachung:* Die fehlerhafte Anmeldung am PC wird systemseitig protokolliert. Das Protokoll ist regelmäßig von dem Administrator oder dem Datenschutzbeauftragten auszuwerten.

Untersuchungen haben ergeben, dass ein erheblicher Teil von Missbrauchsfällen dadurch verursacht wurde, dass der „Einbruch“ über normale Benutzerkennzeichen erfolgte, deren Passworte erraten oder ausgekundschaftet wurden.

Die Verantwortung für die Bildung und Verwendung des individuellen Passwortes liegt bei jedem einzelnen Benutzer!

Tipps für die Bildung und Verwendung von Passwörtern!



- *Verwenden Sie Zeichen aus den folgenden drei Gruppen:*
  1. *Buchstaben, z. B. A, B, C... und a, b, c...,*
  2. *numerische Zeichen, z. B. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,*
  3. *Symbole (alle Zeichen außer Buchstaben und numerische Zeichen), z. B. ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /.*
- *Benutzen Sie nur Passwörter, die aus mindestens 6 Zeichen bestehen.*
- *Ändern Sie Ihr Passwort regelmäßig (Tasten Strg + Alt + Entf). Bei Verdacht auf Missbrauch informieren Sie unverzüglich Ihren Fachvorgesetzten.*
- *Halten Sie Ihr Passwort geheim. Geben Sie das Passwort nicht an Kollegen oder an Administratoren weiter.*
- *Schreiben Sie Ihr Passwort nicht auf einen Zettel, den sie im Büro unverschlossen aufbewahren.*
- *Geben Sie Ihr Passwort auch nicht telefonisch an Personen weiter, die sich als Administratoren oder Vorgesetzte ausgeben.*
- *Speichern Sie Ihr Passwort nicht auf programmierbaren Funktionstasten oder in einer Datei.*

Passwörter, die leicht "ausgespäht" werden können:

- *Namen von Ortschaften (Kiel01, HAMBURG), Geburtsdaten (01011960, 01.01.60, 10/01/60), Auto- und Telefonnummern (KI-XY-123, 6399393).*
- *(Vor-)Namen von Freund(inn)en und Haustieren, z. B.: Ellen, EMeier, Harry, Bello, Hasso, Birdy.*
- *Passwortgenerationen, wie stephan1, stephan2 usw., bieten ebenfalls nicht den nötigen Schutz.*

- *Begriffe, die im Lexikon vorkommen, lassen sich leicht erraten. Passwortcrackprogramme durchsuchen z. B. zunächst Übereinstimmungen mit Wörtern aus Lexika.*
- *Auch simple Folgen von Zahlen oder Buchstaben wie 1234567, aaaaaaa oder qwertzi sind leicht zu erraten bzw. zu hacken.*

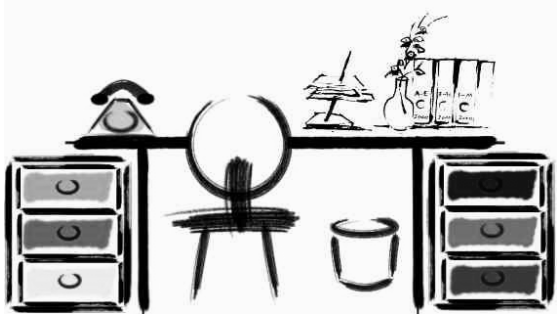
Passwörter, die Sie einsetzen sollten:

- *Bilden Sie ein Passwort mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen, z. B. Pa"!woR oder q9_Er§3.*
- *Wählen Sie ein beliebiges Wort (Achtung: Wortlänge!), ersetzen Sie einzelne Buchstaben durch Sonderzeichen/Zahlen und kombinieren Sie Groß- und Kleinschreibung. So können Sie z. B. das Wort "Passwort" abwandeln, indem Sie das "a" durch @, das "o" durch & ,das "ss" durch 2s ersetzen und Groß- und Kleinschreibung kombinieren. Sie erhalten P@2sW&rT.*
- *Sie können z. B. auch aus einem Sprichwort oder Schlagertitel ein Passwort erstellen. Nehmen Sie z. B. den Schlager "Ohne Krimi geht die Mimi nie ins Bett...": Die Anfangsbuchstaben der Wörter ergeben unter Berücksichtigung der Groß- und Kleinschreibung: OKgdMniB. Ersetzen Sie noch ein oder zwei Zeichen durch Zahlen und/oder Sonderzeichen und Sie erhalten z. B. O%gdMn1B*

Passwörter, die Sie auf diese oder ähnliche Weise erzeugen, lassen sich nur sehr schwer erraten. Auch gute Passwortcrackprogramme brauchen sehr lange, bis sie solche Passwörter geknackt haben.

Je **mehr Mitarbeiter** in einer Organisation arbeiten, desto **größer** ist die **Wahrscheinlichkeit**, dass eigene Mitarbeiter die Passwörter ihrer Kollegen ausspähen. Sie können für einen leichtfertigen Umgang mit Ihrem Passwort und einen daraus resultierenden Schaden zur Verantwortung gezogen werden.

4. Benutzeroberfläche



Wie organisieren Sie sich Ihren Arbeitsbereich an Ihrem Schreibtisch? Dort finden sich sicher alle die Arbeitsmaterialien, die Sie zur Erfüllung Ihres Aufgabengebietes benötigen, z. B. Schreibblock und Stifte, Telefon, Vordrucke, Ordner usw.. Übertragen Sie diese Organisation Ihres Arbeitsplatzes auf den Computer!

Nachdem Sie sich am System angemeldet haben, sehen Sie Ihren persönlichen "Desktop" (Schreibtisch) auf Ihrem Bildschirm. Je nachdem welches Betriebssystem (Windows 95/98, NT Workstation, 2000 Professional, XP) Ihre Organisation einsetzt, können diese Desktop-Oberflächen unterschiedlich gestaltet sein. Über diese Benutzeroberfläche sollten Sie auf alle Programme und Funktionen zugreifen können, die Sie für Ihren Aufgabenbereich benötigen.

Betrachten Sie Ihre Benutzeroberfläche kritisch und prüfen Sie, ob Sie alle Programme und Funktionen auch wirklich benötigen.

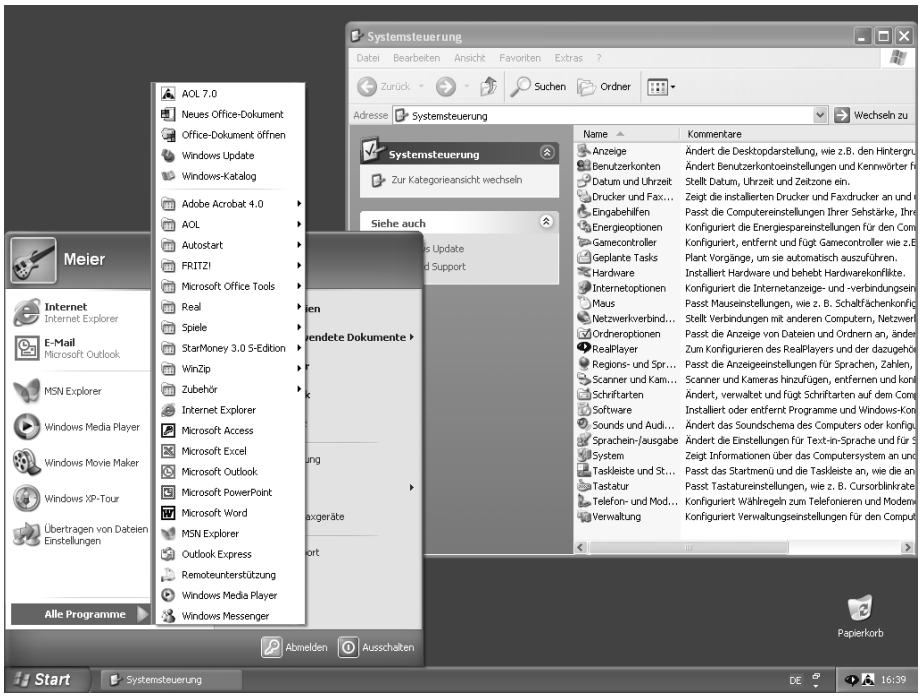


Abb.: Windows XP – Standardbedieneroberfläche ohne Funktionseingrenzung

Sieht Ihre Benutzeroberfläche vielleicht sogar wie oben abgebildet aus? Sollte das der Fall sein, dann können Sie davon ausgehen, dass Ihre Benutzeroberfläche nicht an Ihr Aufgabengebiet angepasst worden ist. Für Sie bedeutet das, dass Sie auf Systemfunktionen Zugriff haben, auf die eigentlich nur die Administratoren zugreifen sollten.

Wird ein Betriebssystem auf einem PC installiert, so haben Benutzer **standardmäßig Zugriff** auf viele Programme und Systemfunktionen. Das birgt für den Benutzer die Gefahr, dass er unwissentlich Einstellungen vornimmt, die die **Sicherheit des Systems** beinträchtigen können und für die er im schlimmsten Fall auch zur Verantwortung gezogen werden kann.

Daher sollten die Administratoren in Anlehnung an das Sicherheitskonzept und evtl. in Absprache mit Ihrem Fachvorgesetzten die Benutzeroberfläche so gestalten, dass Sie nur auf die für Ihr Aufgabengebiet benötigten Programme und Funktionen zugreifen können.

Berücksichtigt der Administrator bei der Erstellung Ihres Benutzerkontos keine Funktionseinschränkungen, verfügen Sie **standardmäßig** über zahlreiche Administrationswerkzeuge und erhalten somit indirekt eine Administratorfunktion.

Wie sollte meine Benutzeroberfläche nicht aussehen?

Die Datensicherheit auf Ihrem Arbeitsplatz-PC ist unzureichend, wenn Sie z. B.

- *die Eingabeaufforderung (START-PROGRAMME-ZUBEHÖR-EINGABEAUFFORDERUNG),*
- *die Funktion Ausführen (START-AUSFÜHREN),*
- *die Funktion Systemsteuerung (z. B. START-EINSTELLUNGEN-SYSTEMSTEUERUNG oder unter Arbeitsplatz),*
- *die Funktion Netzwerkumgebung (z. B. auf dem Desktop oder im Explorer) und/oder*
- *den Explorer (z. B. Klick mit der rechten Maustaste auf START-EXPLORER) uneingeschränkt benutzen können*

oder über die Benutzeroberfläche auf ein Disketten- und/oder CD-ROM-Laufwerk dauerhaft zugreifen können.

Wie bekomme ich eine Benutzeroberfläche, die zu meinem Aufgabengebiet passt?

Möchten Sie sichergehen, dass die Datensicherheit auf Ihrem Arbeitsplatz-PC gewährleistet ist, dann

- *überprüfen Sie den Funktionsumfang Ihrer Benutzeroberfläche, berücksichtigen Sie auch die oben aufgeführten Punkte,*
- *überlegen Sie, welche Programme und Funktionen Sie für Ihre Arbeitsabläufe benötigen und dokumentieren Sie diese,*
- *suchen Sie das Gespräch mit Ihrem Fachvorgesetzten und dem Administrator und machen Sie sie darauf aufmerksam, dass bei unzureichenden Sicherheitsmaßnahmen auf dem Arbeitsplatz-PC ein Verstoß gegen die Datenschutzbestimmungen vorliegt,*
- *legen Sie Ihrem Fachvorgesetzten und dem Administrator dar, welche Programme und Funktionen Sie benötigen, so dass der Administrator Ihre Benutzeroberfläche entsprechend zuschneiden kann.*

5. Datenablage

Kehren wir noch einmal zur papierenen Datenverarbeitung zurück. Können Sie von sich behaupten, dass Sie alle Akten und Vorgänge, die Sie bearbeitet haben, wiederfinden? Wenn ja, dann haben Sie Ihre Datenbestände und Ordner gut strukturiert. Vielleicht hat Ihnen Ihre Organisation auch eine Ablagestruktur vorgegeben und Sie in deren Gebrauch eingewiesen. Auch diese strukturierte Verwaltung von Datenbeständen lässt sich auf die automatisierte Datenverarbeitung übertragen.

Wie Sie im Verlauf des Kapitels noch sehen werden, können Daten (Textdokumente, Tabellen) **relativ leicht unstrukturiert** auf den Festplatten des Servers oder sogar auf der lokalen

Festplatte des Arbeitsplatz-PC abgelegt werden. Dabei besteht die Gefahr, dass die Mitarbeiter und die Verantwortlichen schnell den **Überblick** über diese Datenbestände **verlieren** und ggf. unberechtigte Personen auf sie zugreifen können. Auch die Datensicherung wird durch eine unstrukturierte Datenspeicherung erschwert. Normalerweise werden Datenbestände auf den Servern in regelmäßigen Abständen gesichert. Werden Datenbestände aber lokal auf der Festplatte des Arbeitsplatz-PC gespeichert, werden diese nicht in die Datensicherung mit einbezogen. Im schlimmsten Fall muss bei Systemfehlern mit dem Verlust der lokalen Datenbestände gerechnet werden.

Eine **zentrale Ablage** bietet die Möglichkeit, die Datenbestände strukturiert und überschaubar zu speichern. Dabei wird für jeden Mitarbeiter auf dem Server ein bestimmter Bereich zur Verfügung gestellt, den er zur Speicherung seiner Datenbestände nutzen kann. Dieser Ablagebereich wird durch den Administrator durch Zugriffsrechte so abgeschottet, dass nur autorisierte Mitarbeiter oder Fachvorgesetzte auf diesen Bereich zugreifen können (siehe Kapitel 6). Ein Beispiel für eine zentrale Ablage zeigt die nachfolgende Abbildung:

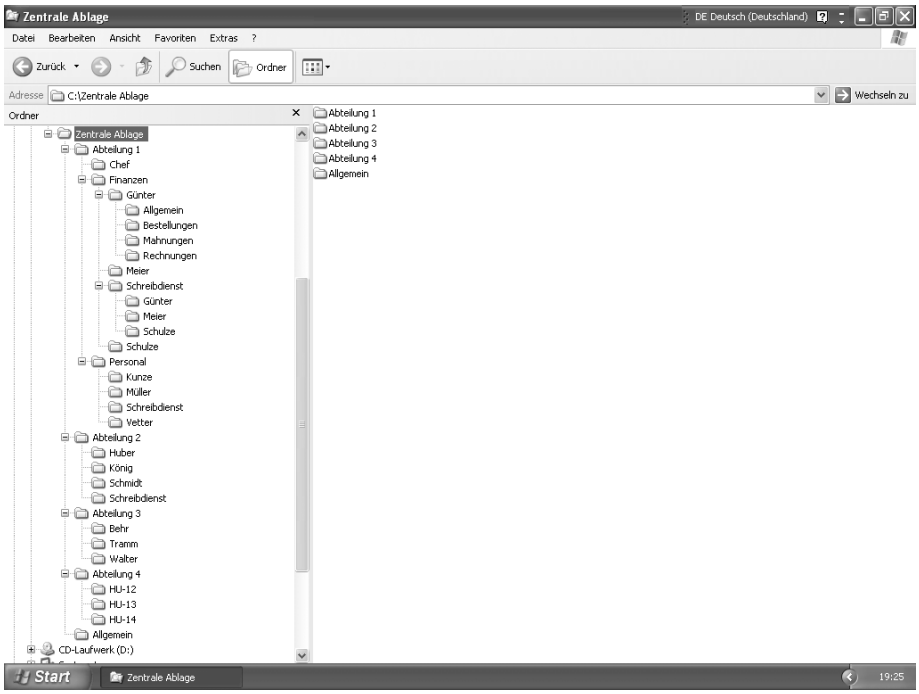
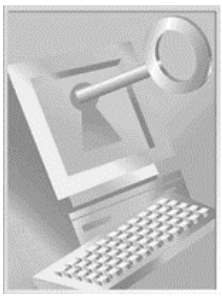


Abb.: Struktur einer zentralen Ablage

Welche Vorteile bietet eine zentrale Datenablage?



Sie bietet den Vorteil, dass

- *sie eine einfache und effektive Möglichkeit zur Verbesserung der Datensicherheit am Arbeitsplatz darstellt,*
- *nur autorisierte Mitarbeiter (z. B. Vertretung) und Fachvorgesetzte auf Ihren Ablagebereich zugreifen dürfen,*
- *Sie die Übersicht über Ihren Datenbestand nicht verlieren und ihn besser verwalten können; so können Sie z. B. Ihre Ablage leicht aufräumen, indem Sie nicht mehr benötigte Dateien löschen (damit ist auch der Grundsatz der Datensparsamkeit und Datenvermeidung gewährleistet).*

Wie sollte die Datenablage nicht aussehen?

- *Es gibt keinen zentralen Ort für die Ablage.*
- *Sie können auf die Daten Ihrer Kollegen zugreifen, auf die Sie eigentlich keinen Zugriff haben dürften.*
- *Ablageordner, die vom Administrator oder von Mitarbeitern selbst erstellt worden sind, liegen "verstreut" auf dem System.*
- *Es befinden sich Daten und Ordner auf der lokalen Festplatte Ihres Arbeitsplatz-PC.*

So sollte eine Datenablage auf meinem System aussehen!

- *Eine zentrale Ablage ist eingerichtet worden.*
- *Die zentrale Ablage ist nach Abteilungen, Aufgabengebieten oder organisatorischen Strukturmerkmalen eingerichtet.*
- *Die Ablage kann auch eine erweiterte Unterstruktur aufweisen, z. B. durch Namen oder Geschäftszeichen.*
- *Für jeden Mitarbeiter ist ein Ordner bereitgestellt worden.*

- *In Ihrem Ordner können Sie eigenständig eine Unterstruktur anlegen, die Ihrem Aufgabengebiet entspricht.*
- *Außerhalb Ihres Ordners dürfen Sie keine Veränderung an der Struktur der Ablage vornehmen.*
- *Ihr Ordner ist gegen den Zugriff Ihrer Kollegen geschützt und Sie können nicht auf die Ordner Ihrer Kollegen zugreifen.*
- *Gibt es in Ihrer Organisation einen zentralen Schreibdienst, so sollte er abteilungsbezogen in die zentrale Ablage eingegliedert werden. Beachten Sie, dass die Verantwortung für das Schreibgut (Dateien) bei dem jeweiligen Auftraggeber (Mitarbeiter) liegt.*

Wissen Sie eigentlich, **wo Ihre Daten gespeichert** werden, wenn Sie den Befehl SPEICHERN ausführen? Das kann, je nach dem welche Software Sie benutzen, durchaus unterschiedlich sein.

Arbeiten Sie mit einer **speziellen Fachanwendung**, dann haben Sie in der Regel keinen Einfluss darauf, wo die Daten gespeichert werden. Stellen Sie sich folgende Situation vor: Sie und mehrere Ihrer Kollegen arbeiten mit der gleichen Fachanwendung und greifen auf die gleiche Datenbank zu, die auf einem Server installiert ist. Alle Daten, die Sie erfassen, bearbeiten oder löschen, werden in dieser Datenbank (auf dem Server) verwaltet. Damit diese Daten im Falle eines Systemausfalls wiederhergestellt werden können, werden sie in regelmäßigen Abständen auf einem Datenträger (Magnetband etc.) gesichert. Eine ordnungsgemäße Datensicherung und ein Mehrplatzzugriff kann nur gewährleistet werden, wenn alle Daten zentral an einer Stelle verwaltet werden. Daher ist der Speicherort bei der Installation fest vorgegeben.

Arbeiten Sie hingegen mit einer **Standardsoftware**, wie z. B. Microsoft Office, dann müssen Sie sich vor dem Speichern Ihrer Dokumente überlegen, in **welchem Ordner** Sie diese ablegen möchten.

Das hat folgenden Hintergrund: Die Standardsoftware ist auf eine große Anzahl von Benutzern ausgerichtet, die mit **unterschiedlichen Computern** und **Betriebssystemen** arbeiten. Wird nun z. B. Microsoft Word mit der Standardkonfiguration installiert, so wird bei allen

Dateien, die Sie erstmals mit SPEICHERN ablegen möchten, der **Ordner EIGENE DATEIEN** als **Standardspeicherort** vorgeschlagen.

Bei jedem Betriebssystem, auf dem Microsoft Word installiert werden kann, existiert dieser **Ordner EIGENE DATEIEN** immer an der gleichen Stelle, nämlich auf der **lokalen Festplatte**, d.h. auf dem Arbeitsplatz-PC unter Ihrem Schreibtisch. Somit ergibt sich das Problem, dass die Datenbestände auf dem lokalen Arbeitsplatz-PC abgelegt werden und nicht in die Datensicherung einbezogen werden. Die Abbildung zeigt den Standardablageordner bei dem Betriebssystem Windows XP Professional.

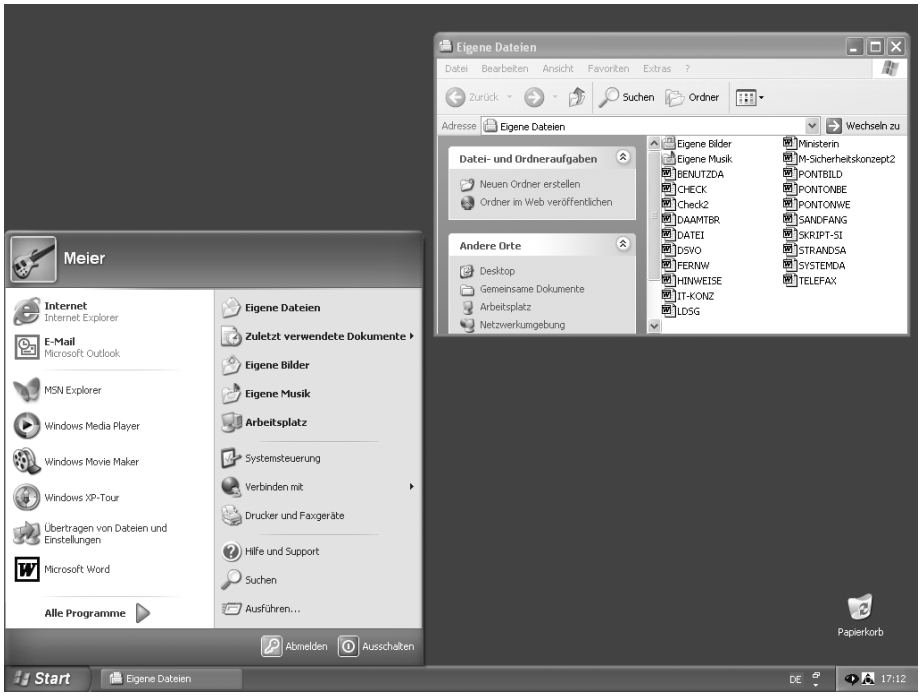


Abb.: Ablageordner EIGENE DATEIEN

Sie können Ihre Daten und Dateien aber nicht nur in dem Standardablageordner EIGENE DATEIEN, sondern auch in jedem anderen Ordner, auf den Sie zugreifen dürfen, abspeichern. Über die **Option SPEICHERN UNTER** können Sie Ihren **bevorzugten Speicherort** wählen. Das hat den Vorteil, dass Sie Ihre Daten gezielt in Ihrem Ordner der zentralen Ablage abspeichern können. Nutzen Sie die Option SPEICHERN UNTER allerdings dazu, um Ihre Daten "mal hier und mal dort" abzulegen, kann das wiederum zu einer **unkontrollierten** und **unstrukturierten Datenablage** führen, die mit ziemlicher Sicherheit ins *Datenchaos* führt.

Um ein solches *Datenchaos* zu verhindern, haben Sie bei der Standardsoftware die Möglichkeit, den bevorzugten Speicherort für Ihre Dateien vorzugeben. So können Sie z. B. bei Microsoft Word über das Menü EXTRAS-OPTIONEN-SPEICHERORT FÜR DATEIEN den bevorzugten Speicherort von dem Ordner EIGENE DATEIEN auf Ihre zentrale Ablage verlegen. Die nachfolgende Abbildung zeigt Ihnen die Einstellmöglichkeit bei Microsoft Word XP.

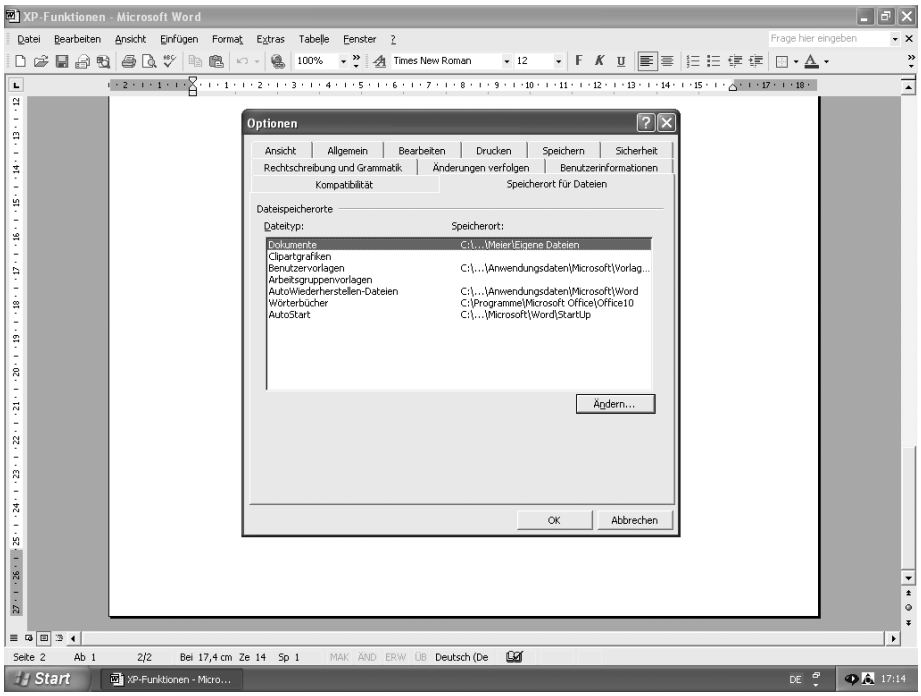


Abb.: Word XP EXTRAS–OPTIONEN–SPEICHERORT FÜR DATEIEN

Das sollten Sie beim Einsatz von Standardsoftware beachten!

- *Überprüfen Sie, in welchem Ordner Ihre Dateien standardmäßig gespeichert werden.*
- *Soll der standardmäßige Speicherort aus bestimmten Gründen nicht geändert werden, dann speichern Sie die Dateien mit der Option SPEICHERN UNTER in Ihrem Ordner der zentralen Ablage.*
- *Werden Ihre Dateien in dem Ordner EIGENE DATEIEN lokal auf Ihrer Festplatte gespeichert, dann kopieren Sie die schon in diesem Ordner vorhandenen Dateien in Ihre zentrale Ablage und ändern Sie den standardmäßigen Speicherort.*

- *Überprüfen Sie Ihre Dateien in Bezug auf die Einhaltung der Speicherfristen und löschen Sie die Dateien, die Sie nicht mehr benötigen.*
- *Berücksichtigen Sie, dass alle in der Organisation erzeugten Datenbestände der Organisation gehören, d.h. es gibt keine privaten Datenbestände. Die Leitungsebene hat also das Recht, sich alle Daten anzusehen. Eine Ausnahme liegt vor, wenn Ihnen die private Nutzung Ihres Arbeitsplatz-PC ausdrücklich erlaubt wurde.*
- *Mit der Standardsoftware (z. B. Microsoft Excel und Access) können Sie leicht Listen, Tabellen und auch kleinere Anwendungen (z. B. mit VBA) erstellen. Beachten Sie, dass Sie selbst entwickelte Programme zur Verarbeitung personenbezogener Daten auf Ihrem Arbeitsplatz-PC nur mit Genehmigung Ihres Fachvorgesetzten einsetzen dürfen.*

6. Zugriffsberechtigungen

Haben wir in dem vorherigen Kapitel über die **zentrale Datenablage** und das Abspeichern von Dateien in dieser Ablage gesprochen, so behandelt dieses Kapitel ergänzend das **Absichern** der zentralen Datenablage durch **Zugriffsberechtigungen**. Dieses Thema betrifft Sie als Benutzer nur indirekt, da die Zuständigkeit für die Vergabe der Zugriffsberechtigungen bei Ihrem Fachvorgesetzten liegt und der Administrator die entsprechenden Einstellungen am System vornimmt. Dennoch soll an dieser Stelle auf dieses Thema eingegangen werden, da die **richtige Vergabe** der Zugriffsberechtigungen als das **A und O der Datenabschottung** anzusehen ist.

Gehen wir erneut von der papierenen Datenverarbeitung aus: Sie arbeiten mit **personenbezogenen Daten**, die Sie in Ordnern ablegen und in einem abschließbaren Schrank gesondert sichern. Für diesen Schrank haben nur Sie und Ihr Fachvorgesetzter einen Schlüssel. Im Vertretungsfall, bei Krankheit und Urlaub verfügt auch ein weiterer Kollege über einen Schlüssel. Sie haben in Ihrer Abteilung hierdurch Vorsichtsmaßnahmen getroffen, damit keine unbefugten Personen Einblick in die Daten nehmen oder sie gar verändern oder entwenden können.

Doch wie kann der **Zugriff** auf **personenbezogene Daten** in der **zentralen Datenablage** auf dem Server gesteuert werden? Würden Sie bemerken, wenn eine unberechtigte Person auf Ihre Dateien zugreift?

Sie können davon ausgehen, dass Sie den Zugriff nicht bemerken, vor allem, wenn Ihre Dateien nur gelesen und nicht verändert werden.

Doch was sind nun Zugriffsberechtigungen?

Mit den **Zugriffsberechtigungen** steht dem Administrator ein Instrument zur Verfügung, mit dem er nach Vorgabe des Fachvorgesetzten regeln kann, **welcher Benutzer** oder welche Benutzergruppe auf welchen **Ordner zugreifen** darf. Das ist in der papierenen Datenverarbeitung damit zu vergleichen, wer einen Schlüssel zu einem bestimmten Schrank mit Daten erhält und wer nicht. Zugriffsberechtigungen können übrigens nicht nur auf Ordner sondern auch auf Fachanwendungen vergeben werden. Während Sie z. B. das Recht erhalten haben, die Fachanwendung A und die Standardanwendung Word zu nutzen, hat Ihr Kollege vielleicht "nur" das Recht, Word auszuführen. Wie Sie aber schon im Kapitel 4 gelesen haben, wird der Zugriff auf Anwendungen zusätzlich dadurch eingeschränkt, dass dem Benutzer nur die Anwendungen auf seiner Arbeitsoberfläche zur Verfügung stehen, die er für sein Aufgabengebiet benötigt.

Die **Entscheidung**, welcher Benutzer oder welche Benutzergruppe welche Zugriffsberechtigungen auf welche Daten oder Anwendungen erhält, darf der **Administrator nicht eigenverantwortlich** fällen. Der **Fachvorgesetzte** (Datenverantwortliche) legt fest, welche Zugriffsberechtigungen seine Mitarbeiter erhalten. Der Administrator setzt die Rechtevergabe auf Weisung des Datenverantwortlichen technisch um.

Je **größer** die Organisation ist, desto **umfangreicher** werden die Aufgaben des Administrators, d.h. es müssen mehr Benutzerkonten verwaltet, die Zugriffsrechte differenzierter vergeben und umfangreichere Anwendungen installiert und gepflegt werden. Dadurch erhöht sich das **Risiko**, dass **Fehler** bei der Vergabe der Zugriffsberechtigungen auftreten können.

Deshalb sollten die Datenverantwortlichen und Administratoren folgende Regeln beachten:

- Die Datenverantwortlichen sollten die Zugriffsberechtigungen ihrer Mitarbeiter schriftlich festlegen und dem Administrator zur Ausführung vorlegen.
- Der Administrator sollte die Vergabe der Zugriffsberechtigungen dokumentieren.
- Die Datenverantwortlichen und/oder der Datenschutzbeauftragte sollten die Systeme in regelmäßigen Abständen auf die ordnungsgemäße Vergabe der Zugriffsberechtigungen überprüfen.

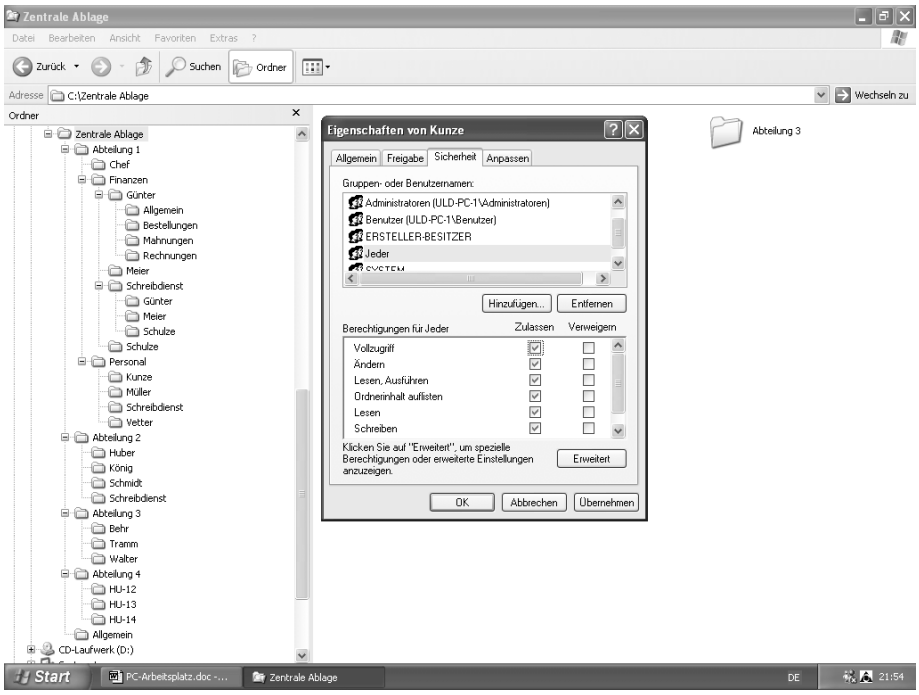


Abb.: Zugriffsberechtigungen Zentrale Ablage, Mitarbeiter Kunze

Was sollte ich über Zugriffsberechtigungen wissen?

Bei der Vergabe von Zugriffsberechtigungen haben Sie als Mitarbeiter keine Entscheidungsbefugnis. Sie können aber

- *an Ihrem Arbeitsplatz-PC überprüfen, auf welche Ordner und Anwendungen Sie selber zugreifen dürfen,*

- *an Ihrem Arbeitsplatz-PC überprüfen, ob Sie auf Ordner von Kollegen anderer Fachabteilungen zugreifen können, in die Sie eigentlich keinen Einblick haben dürften,*
- *den Datenverantwortlichen oder den Administrator informieren, wenn Sie zu weit gehende Zugriffsberechtigungen bemerken und*
- *das Gespräch mit Ihrem Fachvorgesetzten, dem Datenschutzbeauftragten oder dem Administrator suchen, wenn Sie feststellen, dass in Ihrer Organisation Daten nicht hinreichend durch Zugriffsberechtigungen abgeschottet werden.*

7. Disketten- und CD-ROM-Laufwerke

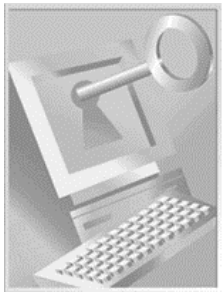
Warum stellen **aktive** Disketten- und CD-ROM-Laufwerke grundsätzlich ein **Sicherheitsrisiko** dar?

Ein Disketten- und CD-ROM-Laufwerk gehört zu der Ausstattung eines Standard-PC. Diese Laufwerke bieten den Benutzern vielfältige Funktionalitäten, doch innerhalb einer Organisation gefährden sie die getroffenen Sicherheitsmaßnahmen. So lassen sich beispielsweise mithilfe von Disketten und CD-ROMs personenbezogene Daten zwischen PC austauschen. Es besteht jedoch die Gefahr, mit diesen Datenträgern Viren einzuschleusen, die sich auch auf andere IT-Systeme ausbreiten.

Selbst wenn Ihre Organisation viel Aufwand betreibt, die IT-Systeme optimal zu schützen, so kann sie wenig gegen die Programme und Daten ausrichten, die mithilfe von Disketten und CD-ROMs eingeschleust werden.

Die Gefahr liegt nicht nur in der Vireninfektion. Es können auch Programme in das System eingespielt werden, die z. B. Lizenzvereinbarungen verletzen, die Systemeinstellungen beeinträchtigen oder sogar zum Datenverlust führen. Ein weiteres Sicherheitsrisiko ist der Einsatz von Hackersoftware. Der dadurch entstehende Schaden kann sehr hoch werden.

Überlegungen zu Disketten- und CD-ROM-Laufwerken:



Aktive (offene) Disketten- und CD-ROM-Laufwerke

- *sind als ein hohes Sicherheitsrisiko einzustufen,*
- *können zu einem hohen Schaden führen,*
- *sollten nur die Mitarbeiter benutzen, die diese Laufwerke für Ihr dienstliches Aufgabengebiet zwingend benötigen und*
- *sollten bei Arbeitsplätzen, an denen Laufwerke nicht benötigt werden, mit technischen Maßnahmen deaktiviert werden.*

Folgende Sicherheitsmaßnahmen stehen dem Administrator zur Verfügung, um an Ihrem Arbeitsplatz-PC das Disketten- und CD-ROM-Laufwerk zu deaktivieren:

- Die Ausrüstung aller PC-Arbeitsplätze mit **Disketten- bzw. CD-ROM-Schlössern** kann je nach Anzahl der auszurüstenden PC sehr teuer werden und ist zudem nicht besonders sicher. Da die Schlösser im freien Handel verfügbar sind, sind Ersatzschlüssel relativ einfach zu erhalten, so dass ein nicht autorisierter Mitarbeiter unbemerkt ein Schloss öffnen könnte. Gleichwohl kann diese Lösung für Einzelplatz-PC oder für Laptops geeignet sein.
- Die Deaktivierung des Diskettenlaufwerkes im so genannten **BIOS** bzw. die **Deaktivierung** der **Disketten- und CD-ROM-Laufwerke-Dienste** ist eine sehr wirkungsvolle Lösung. Allerdings ist bei einer Administration des PC das Disketten- und/oder das CD-ROM-Laufwerk wieder zu aktivieren. Im Ergebnis ist also auch dies keine optimale Lösung, jedoch sicherer als die „Schlosslösung".
- Der Einsatz einer speziellen **Sicherheitssoftware**, die benutzer- oder gruppenbezogen Disketten- und CD-ROM-Laufwerke verschließt oder freigibt, ist zweifellos die effektivste Sicherheitsmaßnahme. Sie ist mit wenig Know-how zentral über das Netz zu administrieren und kann problemlos an spezifische Benutzeranforderungen angepasst werden. Die folgende Abbildung zeigt das Administrationsfenster von der Sicherheitssoftware *DeviceLock.*

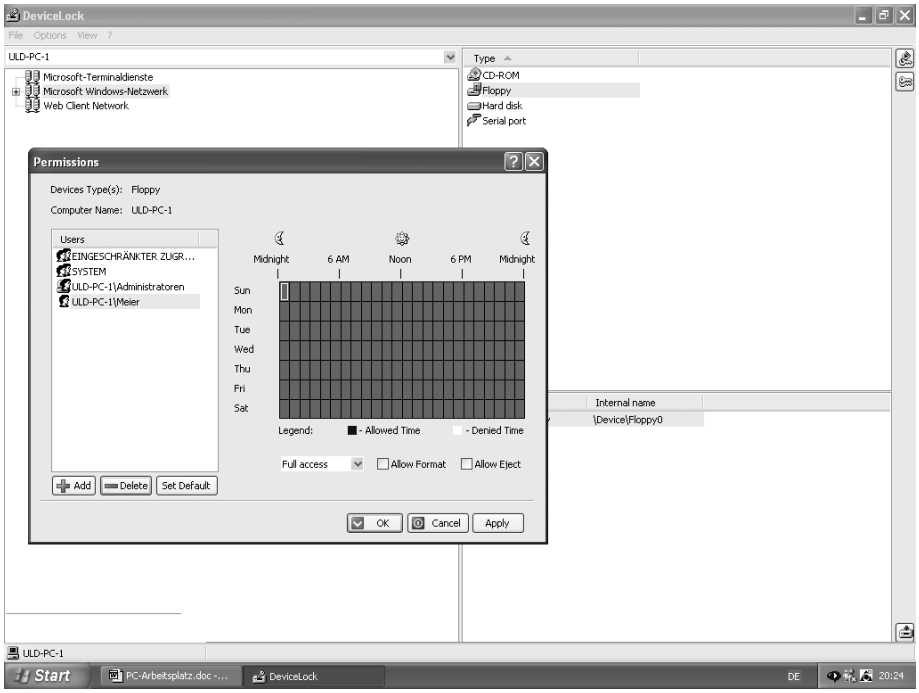


Abb.: Sicherheitssoftware Devicelock

Beachten Sie auch die Neuentwicklungen, die im EDV-Bereich auf den Markt kommen. So können Sie jetzt Speichermedien von 16 MB bis zu 2 GB an den **USB-Anschluss** eines PC anschließen. Auch wenn die Disketten- und CD-ROM-Laufwerke optimal verschlossen sind, können diese Speichermedien ohne Installation von Software an den Rechner angeschlossen werden und wie eine transportable Festplatte benutzt werden. Aus diesem Grund muss auch der USB-Port deaktiviert bzw. gesperrt werden.

Was muss ich bei einem offenen Disketten- und/oder CD-ROM-Laufwerk beachten:

Benötigen Sie für Ihre dienstlichen Aufgaben ein aktives Disketten- und CD-ROM-Laufwerk, dann sollten Sie

- *jedes Speichermedium (Diskette, CD-ROM) vor der Benutzung auf Virenbefall überprüfen, bzw. vom Administrator überprüfen lassen,*
- *keine eigenen Programme und/oder Tools von externen Speichermedien auf Ihren Arbeitsplatz-PC einspielen,*

- *Ihr Disketten- und CD-ROM-Laufwerk vom Administrator deaktivieren lassen, wenn Sie es längere Zeit nicht benötigen,*
- *keine Personen an Ihrem Arbeitsplatz-PC arbeiten lassen, die dann das Disketten- oder CD-ROM-Laufwerk unbefugt nutzen können.*

8. Textverarbeitung mit Microsoft Word

Ziehen wir im Bereich der Textverarbeitung nochmals einen Vergleich zu der papierenen Datenverarbeitung. Wenn Sie z. B. an einem Schriftsatz arbeiten und ihn an Ihre Kollegen zur Mitbearbeitung weitergeben, so können Sie gegebenenfalls die durchgeführten Änderungen nachvollziehen. Oder Sie verwahren einen Brief, in den Ihre Kollegen keinen Einblick nehmen dürfen, verschlossen auf. In der automatisierten Datenverarbeitung ist die Differenzierung, welcher Kollege ein Dokument nur lesen kann oder zusätzlich auch ändern darf, komplexer.

In den meisten Organisationen wird für die Textverarbeitung die Software Microsoft Word eingesetzt. Word enthält einige Sicherheitsoptionen, die von dem Benutzer aktiviert werden sollten. Die nachfolgende Tabelle zeigt die Sicherheitsoptionen in Abhängigkeit zu der eingesetzten Word-Version:

Sicherheitsoption	**Version**
Schützen eines Dokumentes vor unbefugten Änderungen Sie können für das Öffnen oder Ändern eines Dokumentes ein Pass- bzw. Kennwort vergeben (DATEI-SPEICHERN UNTER-EXTRAS-ALLGEMEINE OPTIONEN). *Kennwort für Ändern:* Originaldokumente können nur von dem Benutzer geändert werden, der über das *Schreibschutz-Kennwort* verfügt. Andere Benutzer können auf das Dokument nur lesend zugreifen.	Ab Word 95

Kennwort für Öffnen: Das Dokument kann nur von dem Benutzer geöffnet werden, der über das *Schreib-/Leseschutzkennwort* verfügt. Das Dokument wird über das Kennwort verschlüsselt abgelegt. Ab Word XP kann der Benutzer verschiedene Verschlüsselungstypen verwenden.	
Dokument schützen Wenn Sie in Ihrem Dokument Änderungen verfolgen möchten, klicken Sie die Option *Änderungen verfolgen* an. Mit der optionalen Vergabe eines Kennwortes erreichen Sie, dass nur Sie diesen Dokumentenschutz aufheben können.	Ab Word XP
Schützen persönlicher Daten Sie können persönliche Daten aus dem Dokument entfernen. Dazu gehören z. B. die Dateieigenschaften (AUTOR, MANAGER, FIRMA UND ZULETZT GESPEICHERT VON).	Ab Word XP
Digitale Signaturen Sie können Dateien mit einer digitalen Signatur versehen, um zu gewährleisten, dass die Datei nicht geändert wurde. Dieses setzt jedoch die Verwaltung von Zertifikaten voraus.	Ab Word XP
Verstärkter Schutz gegen Makroviren Sie können verschiedene Sicherheitsstufen für das Ausführen von Makros auswählen. Entweder werden nur signierte Makros oder Makros unter Angabe der Quelle des Herstellers akzeptiert. Administratoren können darüber hinaus *Visual Basic für Applikationen* - die Programmiersprache von Microsoft Office - deaktivieren, wenn sie Microsoft Office installieren. Dadurch wird das Ausführen von Makros verhindert.	Ab Word XP

Die nachfolgende Abbildung zeigt die Sicherheitsoptionen bei Microsoft Word XP (DATEI-SPEICHERN UNTER-EXTRAS-ALLGEMEINE OPTIONEN).

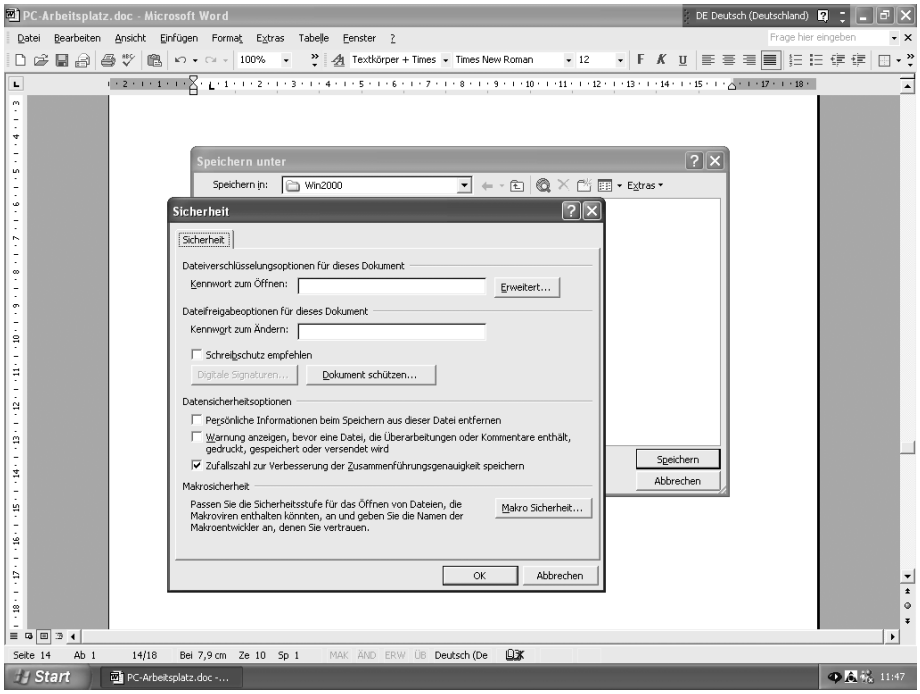
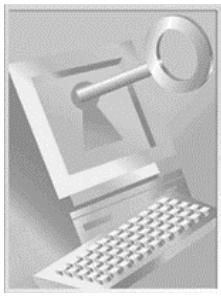


Abb.: Word XP Sicherheitsoptionen

Beachten Sie, dass innerhalb Ihrer Organisation die Administratoren auf den IT-Systemen über Vollzugriffsrechte verfügen. Das bedeutet, dass Administratoren unbemerkt auf Ihre vertraulichen Dokumente zugreifen können (siehe auch nächstes Kapitel).

Durch die Aktivierung der Sicherheitsoptionen schützen Sie Ihre Dokumente!



- *Mit einem Schreib-/Leseschutzkennwort können Sie Ihre Dokumente vor einem unbefugten Zugriff schützen.*
- *Beachten Sie, dass Sie nicht für jedes Dokument ein neues Kennwort vergeben. Das könnte dazu führen, dass Sie später nicht mehr wissen, für welches Dokument Sie welches Kennwort vergeben haben.*
- *Regeln Sie in Ihrer Abteilung die Vergabe von Kennwörtern für Worddokumente. Die Fachvorgesetzten sollten klare Strukturen vorgeben.*
- *Berücksichtigten Sie, dass bei einer Änderung eines einheitlichen Kennwortes alle Worddokumente entsprechend angepasst werden müssen.*

- *Legen Sie für Worddokumente mit sensiblen Daten kurze Löschungsfristen fest.*
- *Stellen Sie unter der Option Makrosicherheit mindestens die Stufe Mittel ein. Dann werden Sie von Word beim Öffnen eines Dokumentes aufgefordert, zu bestätigen, ob ein integriertes Makro ausgeführt werden soll.*

Das sollten sie außerdem über die Sicherheitsoptionen wissen:

- *Dokumente, die mit einem Schreib-/Leseschutzkennwort geschützt werden, werden verschlüsselt auf der Festplatte abgelegt. Der Inhalt des Dokumentes kann nicht durch den Einsatz anderer Textverarbeitungssysteme offen gelegt werden.*
- *Sollten Sie Ihr Kennwort vergessen haben, kann das Dokument nur über ein spezielles "Passwort-Crackprogramm" (z. B. im Internet erhältlich) geöffnet werden.*
- *Sofern Sie Dokumente nur mit einem Schreibkennwort versehen (ein Benutzer kann es lesen, aber nicht verändern), sollten Sie beachten, dass dieses Kennwort ausgelesen werden kann. Das Dokument muss nur mit einem Editor geöffnet werden. Der Editor zeigt neben dem Text zusätzliche Informationen (Header) an, aus denen auch das Kennwort im Klartext hervorgeht.*

Wussten Sie, dass **Word** während der Dokumentenbearbeitung viele Informationen **"unsichtbar" speichert**? Gibt es einen Grund dafür? Ja, denn im Falle eines Systemabsturzes ist Word in der Lage, die Datei aus den unsichtbar gespeicherten Daten zu rekonstruieren und wiederherzustellen. Einige dieser unsichtbaren Daten können Sie aus der Datei auslesen, wenn Sie (wie in der nächsten Abbildung dargestellt) Word starten, DATEI-ÖFFNEN wählen und die entsprechende Datei mit dem Dateityp TEXT AUS BELIEBIGER DATEI WIEDERHERSTELLEN öffnen. Es werden Ihnen dann neben dem "Originaltext" viele weitere Informationen aus dem Dokument angezeigt.

Ein **Sicherheitsrisiko** besteht immer dann, wenn eine **Word-Datei** aus Ihrem Zuständigkeitsbereich in den Zuständigkeitsbereich eines anderen Mitarbeiters oder in den Zuständigkeitsbe-

reich einer anderen Organisation gegeben wird. Dann erhalten die "Kollegen" nicht nur den eigentlichen "Originaltext" sondern zusätzlich auch noch die "Historie" des Dokumentes.

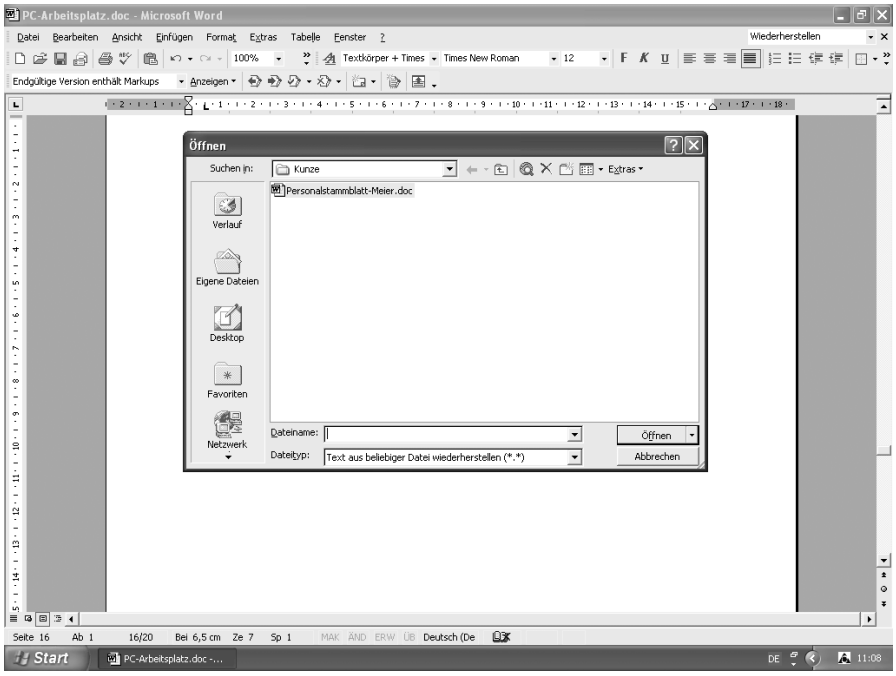


Abb.: Word XP Dokumentenwiederherstellung

Wie gehen Sie nun vor, wenn Sie eine Worddatei weitergeben müssen und verhindern möchten, dass die unsichtbaren Informationen von anderen Personen ausgelesen werden?

1. Sie dürfen die Datei nicht "unbehandelt" weitergeben.
2. Legen Sie zunächst eine leere Worddatei an.
3. Kopieren Sie den Inhalt der Ursprungs-Datei in die neue Datei.
4. Speichern Sie die neue Datei unter einem anderen Namen ab.

Bei diesem Verfahren werden die unsichtbaren Informationen nicht in die "neue" Worddatei übertragen.

Hinweise bei der Weitergabe von Worddateien!

Wenn Sie eine Worddatei an eine andere Fachabteilung oder an eine andere Organisation weitergeben müssen, sollten Sie

- *berücksichtigen, dass die „unsichtbaren" Daten sich innerhalb der Worddatei befinden und auch erhalten bleiben, wenn Sie die Datei auf eine Diskette kopieren oder per E-Mail versenden,*
- *keine „unbehandelten" Word-Dokumente mit personenbezogenen Daten aus Ihrem Zuständigkeitsbereich herausgeben; über die Funktion DOKUMENTENWIEDERHERSTELLUNG können am Text durchgeführte Änderungen rekonstruiert bzw. sichtbar gemacht werden,*
- *die Worddatei insoweit „behandeln", dass der Textinhalt der Ursprungs-Datei in eine neue und leere Worddatei übertragen wird.*

9. (Fern-)Administration

Damit Sie an Ihrem Arbeitsplatz-PC arbeiten können, müssen die **IT-Systeme administriert** werden. Darunter fallen unzählige Aufgaben, z. B. die Verkabelung der PC, die Einrichtung von Benutzerkonten, die Installation und Konfiguration von Fachanwendungen, der Support für die Mitarbeiter usw.. Die Administration wird in der Regel von einem, bei größeren Organisationen von mehreren Administratoren durchgeführt. Vielfach werden auch **externe Dienstleister** mit der Administration beauftragt, die dann von einem entfernten Ort ausgeführt wird (Fernadministration). Da alle Computer in einem Netzwerk miteinander verbunden sind, besteht die Möglichkeit, dass ein Administrator von einem "Administrations-PC" auf **jeden** eingeschalteten Arbeitsplatz-PC zugreifen kann.

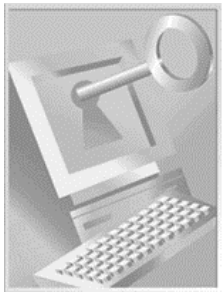
Als **Mitarbeiter** am Arbeitsplatz-PC haben Sie keinen **direkten Einfluss** auf die Administration. Sie sollten aber wissen, dass die Verantwortung für die automatisierte Datenverarbeitung beim Leiter Ihrer Fachabteilung liegt. Deshalb sollte er als Datenverantwortlicher auch festlegen, in welchem Umfang der Administrator auf die Daten Ihrer Abteilung zugreifen darf.

Soll eine Fernadministration z. B. an einer Fachanwendung durchgeführt werden, dann müssen strenge Maßstäbe angesetzt werden. Der Datenverantwortliche muss

- eine Genehmigung zur Fernwartung erteilen und
- über das Ergebnis der Durchführung informiert werden.

Es liegt auch in seiner Entscheidungskompetenz, nach Änderungen an einer Fachanwendung ein erneutes Test- und Freigabeverfahren durchzuführen.

Die Administration der IT-Systeme muss für die Verantwortlichen nachvollziehbar sein!



- *Der administrative oder fernadministrative Zugriff auf personenbezogene Daten der Fachabteilung darf nur mit Einwilligung des Datenverantwortlichen erfolgen.*
- *Die administrativen Tätigkeiten der Administratoren müssen protokolliert und in regelmäßigen Abständen z. B. durch den Datenschutzbeauftragten kontrolliert werden. Diese Maßnahme kann zwischen den Administratoren und Datenbeauftragten Vertrauen schaffen und hat für die Administratoren den Vorteil, dass sie in ihrer Verantwortung entlastet werden.*
- *Die in Ihrer Abteilung eingesetzten Fachanwendungen mit personenbezogenen Daten müssen, bevor sie offiziell eingesetzt werden, zunächst ausreichend getestet und danach von dem Datenverantwortlichen freigegeben werden.*

10. Sicherheit im Internet

Das Internet mit seinen zahlreichen Funktionen ist aus dem modernen Verwaltungs- und Geschäftsleben nicht mehr wegzudenken. So können Sie per elektronischer Post (E-Mail) schnell und unkompliziert Briefe austauschen oder Sie können im World Wide Web (WWW) gezielt nach Informationen suchen.

Sollen diese Dienste von Ihrer Organisation genutzt werden, muss das interne Netzwerk mit dem Internet verbunden werden. Von diesem Moment an ist Ihr IT-System von außen angreifbar und Sie müssen Ihre Daten gegen die Gefahren und Angriffspunkte möglicher Angreifer schützen. Auch Sie können am PC-Arbeitsplatz direkt mit diesen Gefahren konfrontiert werden. Deshalb ist es wichtig, dass Sie diese Gefahren kennen und richtig darauf reagieren.

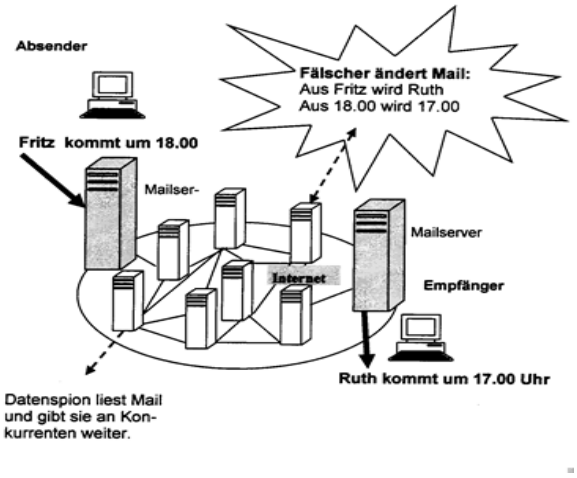
Gefahr durch Hacker

Hacker versuchen möglichst unbemerkt und unerkannt, sich auf Ihrem Computer „einzuschleichen“. Die einfachste Möglichkeit, Zutritt zu Ihrem System zu erhalten, ist der persönliche Kontakt zu den Personen, die Zugriff auf das System haben **(Social Engineering)**. So ist es durchaus denkbar, dass sich jemand bei Ihnen telefonisch als Techniker ausgibt und versucht, von Ihnen Ihr Passwort zu erhalten.

Das Ausspähen der E-Mail-Kommunikation

Die E-Mail-Kommunikation ist unkompliziert und schnell. Doch sie stellt eine unsichere Form der Kommunikation dar. Wenn der Inhalt nicht verschlüsselt ist, können auf dem Weg vom Absender zum Empfänger wichtige Informationen in die falschen Hände gelangen.

Werden zusätzlich der Inhalt der E-Mail oder die Angaben des Absenders verändert, kann der Schaden für Ihre Organisation unter Umständen sehr groß werden. Die nachfolgende Grafik zeigt in vereinfachter Form die verschlüsselte und unverschlüsselte E-Mail-Kommunikation.

unverschlüsselte E-Mail	verschlüsselte E-Mail
	

Die Verschlüsselung bietet Schutz vor dem unberechtigten Lesen und Verändern der E-Mail. Wenn Sie sichergehen möchten, dass auch der angegebene Absender auf der E-Mail dem wirklichen Verfasser entspricht, dann müssen Sie zusätzlich eine digitale Signatur einsetzen. Bei einer digitalen Signatur wird mithilfe eines Signaturschlüsselpaars die Identität des Absenders sichergestellt. Zusätzlich kann rechnerisch festgestellt werden, ob der Inhalt der E-Mail verfälscht worden ist.

Wie verhindere ich ein Ausspähen oder Verändern meiner E-Mails?

Möchten Sie

- *das unbefugte Lesen und Verändern der E-Mail-Inhalte verhindern, dann setzen Sie eine Verschlüsselungssoftware, z. B. PGP, ein,*
- *sichergehen, dass die E-Mail auf dem Weg zum Empfänger nicht gelöscht oder verloren geht, dann vereinbaren Sie mit dem Empfänger ein Empfangsbestätigungsverfahren,*

- *sichergehen, dass der Absender auch wirklich der Verfasser der E-Mail ist und dass keine Veränderung oder Verfälschung am Inhalt oder Absender vorgenommen wurde, dann setzen Sie eine digitale Signatur ein.*

Hoax und Spamming

In jüngster Zeit werden zunehmend falsche Virenwarnungen, sogenannte **Hoax** (englisch: Streich oder übler Scherz), in Form von Kettenbriefen verbreitet. Dabei wird die Angst der Benutzer vor Viren oder Angriffen ausgenutzt. Sie werden durch eine falsche Meldung z. B. aufgefordert

- die Warnung an alle Kollegen und Bekannte zu senden; dabei werden unnötig die Ressourcen der Mailserver verbraucht,
- die Einstellungen Ihres PC durch falsche "Sicherheitstipps" zu verändern; dadurch können Sie allerdings Ihren PC für Angriffe anfälliger machen.

Unter **Spamming** versteht man das unaufgeforderte Zusenden von Werbe-E-Mails. Die Spam-Mail wird von vielen Firmen als Mittel zur Werbung für ihre Produkte eingesetzt. Dabei wird eine Mail an eine große Anzahl von Empfängern versandt (Spam: Send Phenomental Amounts of Mail). Eine andere Art des Spamming liegt vor, wenn eine große Anzahl von E-Mails an eine einzige E-Mail-Adresse gesendet wird. Dabei wird ein E-Mail-Postfach mit Mails "zugebombt", daher wird diese Art des Spamming auch E-Mail-Bombing genannt.

Wie schütze ich mich vor Hoax- und Spam-Mails?

Empfangen Sie an Ihrem Arbeitsplatz-PC

- *Virenwarnungen, mit der Aufforderung diese weiter zu versenden, dann informieren Sie den Administrator, löschen die Mail ungeöffnet und befolgen Sie nicht die „gutgemeinten“ Anweisungen,*
- *Spam-Mails, dann benachrichtigen Sie den Administrator und löschen Sie diese Mails ungeöffnet.*

Beachten Sie weiterhin,

- *dass bei den meisten E-Mail-Verwaltungsprogrammen gelöschte E-Mails zunächst in einen „Papierkorb“ verschoben und erst beim Leeren dieses Papierkorbs endgültig gelöscht werden; deshalb sollten Sie Ihren E-Mail-Papierkorb regelmäßig leeren,*
- *dass Sie Ihre E-Mail-Adresse nicht an jeden weiter geben; so ist die Gefahr geringer, dass Sie mit Spam-E-Mail, o. ä. belästigt werden.*

Gefahr eines Virenbefalls

Der Begriff **Computervirus** ist wohl jedem Computerbenutzer bekannt. Viren können sich von einem Arbeitsplatz-PC über das Computernetz ausbreiten. Eine Vireninfizierung bzw. Virenverbreitung kann auftreten, wenn der Benutzer ein virenverseuchtes Programm aus dem Internet heruntergeladen oder einen virenverseuchten E-Mail-Anhang geöffnet hat.

Ein Virus ist ein Programmsegment, das sich in funktionsfähige „gesunde“ Programme kopiert und nicht erwünschte Funktionen ausführt. Das äußert sich in einem ungewohnten „merkwürdigen“ Verhalten des PC oder gar durch einen Totalausfall. Es gibt eine große Anzahl von unterschiedlichen Computerviren, die sich zudem ständig verändern.

Neben den Computerviren gibt es auch virenähnliche Programme, z. B.

- Trojanische Pferde (Programme, die unerwünschte Funktionen ausführen, die vom Benutzer nicht bemerkt werden, z. B. das Ausspähen von Passwörtern oder Daten) oder
- Logische Bomben (Programme, die erst beim Eintreten eines bestimmten Ereignisses bestimmte Aktionen auslösen, z. B. an einem bestimmten Datum werden alle Word-Dateien gelöscht).

Daher ist ein Virenschutzprogramm mit einer regelmäßigen Aktualisierung unumgänglich.

Wie schütze ich meinen Arbeitsplatz-PC vor einen Virenbefall?

Sie können einen Virenbefall an Ihrem Arbeitsplatz-PC verhindern, indem Sie

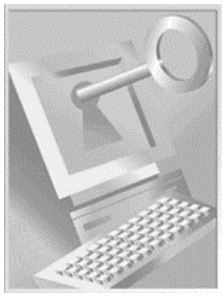
- *alle Disketten, CD-ROMs oder andere Datenträger, die Sie für Ihren Aufgabenbereich benötigen, selbst oder vom Administrator auf Viren prüfen lassen,*
- *suspekte E-Mails, z. B. mit einer offensichtlich unsinnigen Betreffzeile, sofort ungeöffnet löschen; Sie sollten auch misstrauisch werden, wenn Betreffzeilen Wörter wie happy, fun usw. enthalten,*
- *die angehängten Dateien von E-Mails immer mit einem aktuellen Virenschutzprogramm überprüfen bzw. vom Administrator prüfen lassen.*

Die aufgeführten **Sicherheitsrisiken** können auch durch **organisatorische Sicherheitsvorkehrungen** im Bereich der E-Mail-Kommunikation und der Benutzung des World Wide Web verringert werden. Daher sollten Sie als Mitarbeiter im Bereich der Internetnutzung geschult und die Verhaltensregeln sollten detailliert, z. B. in Form einer „Dienstanweisung zur Nutzung der Internetdienste“ (siehe Anhang), festgelegt werden.

Wie können die Sicherheitsanforderungen, z. B. für die E-Mail-Kommunikation, ermittelt werden? Orientieren Sie sich an dem papierenen Briefverkehr, der in den meisten Organisationen bis ins Detail strukturiert und geregelt ist. Überlegen Sie sich, wie Sie diese Regeln auf die E-Mail-Kommunikation übertragen können.

Gibt es in Ihrer Organisation keine Dienstanweisung zur Nutzung der Internetdienste oder keine E-Mail-Dienstanweisung? Dann suchen Sie das Gespräch mit Ihrem Fachvorgesetzten und weisen Sie darauf hin, dass bei gut informierten und geschulten Mitarbeitern die Sicherheitsrisiken deutlich verringert werden können.

Die E-Mail-Kommunikation muss bis ins Detail geregelt sein!



Neben den bereits aufgeführten Sicherheitsmaßnahmen sollten Sie auch folgende Fragen mit Ihrem Fachvorgesetzten klären:

- *Welche E-Mails müssen in den Geschäftsgang gegeben werden?*
- *Welche Daten dürfen nicht Inhalt einer E-Mail sein?*
- *Welche E-Mails müssen ausgedruckt werden?*
- *In welchen Zeitabständen müssen die E-Mails gelöscht werden?*
- *Wer kann im Vertretungsfall auf mein E-Mail-Postfach zugreifen?*
- *Dürfen private E-Mails verschickt werden?*

Dürfen Sie in Ihrer Organisation im **World Wide Web** (WWW) surfen?

Dann müssen die Sicherheitsvorkehrungen auf die Risiken ausgedehnt werden, die dieser Dienst mit sich bringt. Das wird in den meisten Fällen auf zentralen IT-Systemen mit entsprechender Hard- und Software realisiert. Häufig wird auch ein Firewall-System eingesetzt, das das interne Netz zum Internet absichern soll. Diese Absicherung wird bei jedem Netzwerk individuell durchgeführt und ist von vielen Faktoren abhängig, so dass an dieser Stelle nicht näher darauf eingegangen werden kann.

Aber auch bei der Nutzung des WWW können Sie entscheidend zur **Sicherheit** beitragen, indem Sie z. B. die Sicherheitsfunktionen Ihres Browsers (z. B. Internet Explorer oder Netscape Communicator) einsetzen.

Wie aktiviere ich die Sicherheitsfunktionen meines Browsers?

*Verändern Sie die **Sicherheitseinstellungen** des Browsers, indem Sie*

- *das Speichern von **Cookies** auf Ihrem PC deaktivieren; Cookies sind kleine Datenmengen, die vom Betreiber einer Webseite auf Ihrem Rechner gespeichert werden; mithilfe dieser Cookies ist ein Webseitenbetreiber in der Lage, ein Nutzungsprofil von Ihren Surfgewohnheiten zu erstellen; prob-*

lematisch ist, dass Ihnen diese Funktionalität in den seltensten Fällen transparent gemacht wird, d.h. Sie bemerken den Datenaustausch zwischen Ihrem PC und dem Rechner des Webseitenbetreibers nicht,

- ***ActiveX-Komponenten** im Internet Explorer deaktivieren; AciveX ist eine Entwicklung der Firma Microsoft; ActiveX-Komponenten können Dateien auf Ihrem PC auslesen, manipulieren, löschen, Rechner umkonfigurieren oder Viren oder virenähnliche Programme (wie z. B. Trojanische Pferde) installieren; ActiveX-Komponenten stellen ein hohes Sicherheitsrisiko dar,*
- *die **temporären Internet-Dateien**, die Aufschluss über Ihr Surfverhalten geben und in einem speziellen Ordner gespeichert werden, regelmäßig löschen.*

Die nachfolgenden Abbildungen zeigen Ihnen die Optionen für die sicherheitsrelevanten Einstellungen im Internet Explorer des Betriebssystems Windows XP Professional.

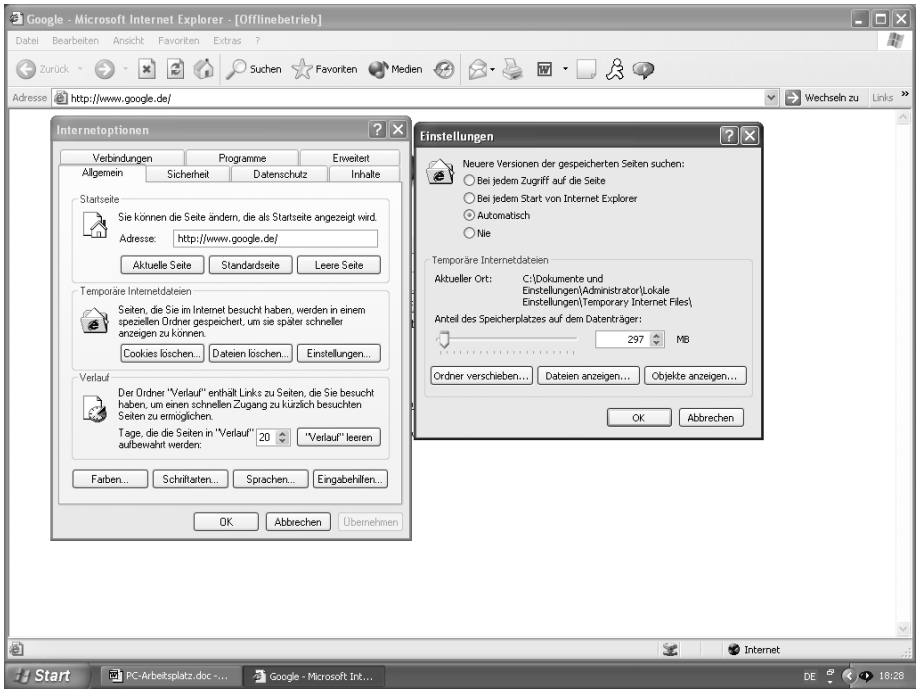


Abb.: Internet-Explorer, Internetoptionen

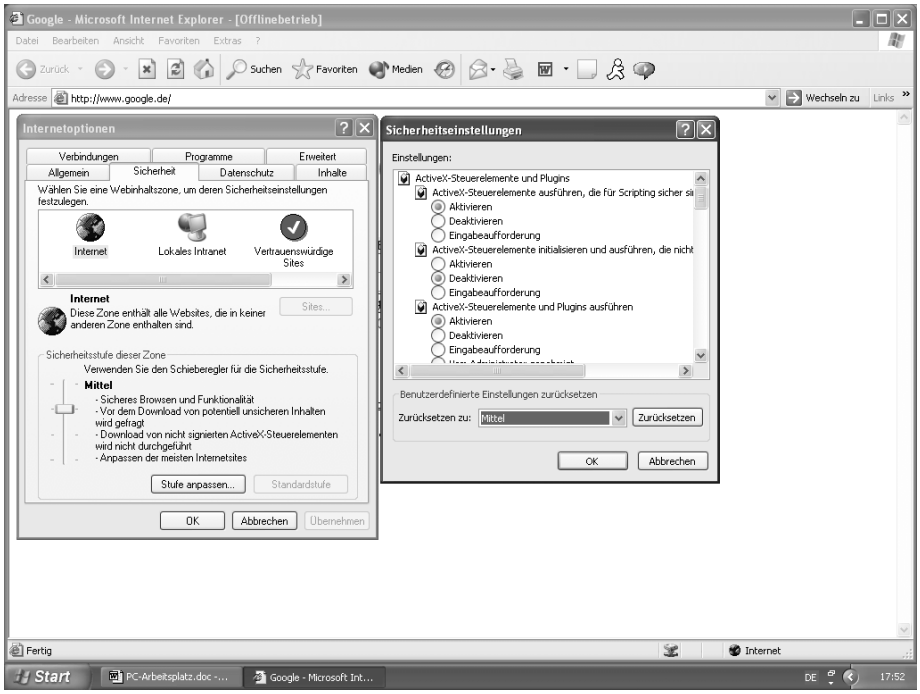


Abb.: Internet-Explorer, Internetoptionen – Sicherheit

Auf der Homepage des Unabhängigen Landeszentrums für Datenschutz (www.datenschutzzentrum.de) erhalten Sie zusätzlich Tipps zum persönlichen Datenschutz bei der Internetbenutzung (unter den Links: Infos für Bürger - Safer Surfen - Selbst sicher(n)!). Dort wird detailliert auf die Gefahren durch ActiveX-Komponenten und Cookies eingegangen.

Beachten Sie beim Surfen im Internet folgende Hinweise!

- *Surfen Sie nur dienstliche Seiten an. Beachten Sie, dass der Administrator durch einen „Webseiten-Blocker" Webseiten blockieren kann, die keinen dienstlichen Bezug haben.*
- *Laden Sie keine Programme oder Dateien aus dem Internet herunter. Falls Sie über eine Download-Funkion verfügen, sollten Sie diese Funktion auf Ihren Arbeitsplatz-PC vom Administrator deaktivieren lassen. Die Download-Funktion stellt ein großes Sicherheitsrisiko dar!*

- *Aktivieren Sie die Sicherheitsfunkionen Ihres Browsers).*
- *Beachten Sie, dass Sie beim Surfen eine Menge Spuren hinterlassen. Auf Ihrem Arbeitsplatz-PC, auf den zentralen Systemen in Ihrer Organisation und dem Provider wird unter anderem festgehalten, welche Web-Seiten Sie aufgerufen haben.*
- *Sie können auch ein Tool für **anonymes Surfen** einsetzen. Informationen hierüber erhalten Sie auf der Homepage des Unabhängigen Landeszentrum für Datenschutz. Bitten Sie Ihren Administrator, dieses Tool für Sie zu installieren.*

Wussten Sie, dass Windows XP automatisch Updates (Neuerungen) aus dem Internet lädt?

Nach der Standardinstallation von Windows XP ist die **Updatefunktion** automatisch aktiviert. Verfügt Ihr PC über einen Internetanschluss, so stellt Windows XP selbstständig eine Verbindung zu einer **Microsoft-Downloadseite** her und überprüft, ob ggf. ein Update für Ihr Betriebssystem vorliegt. Ist dies der Fall, wird es auf Ihren PC übertragen.

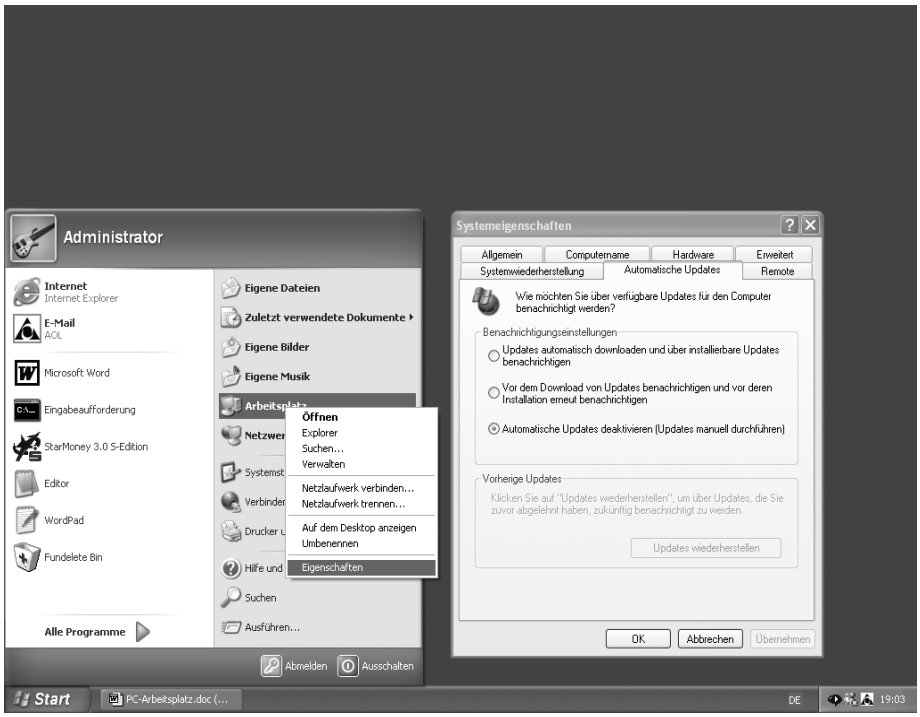
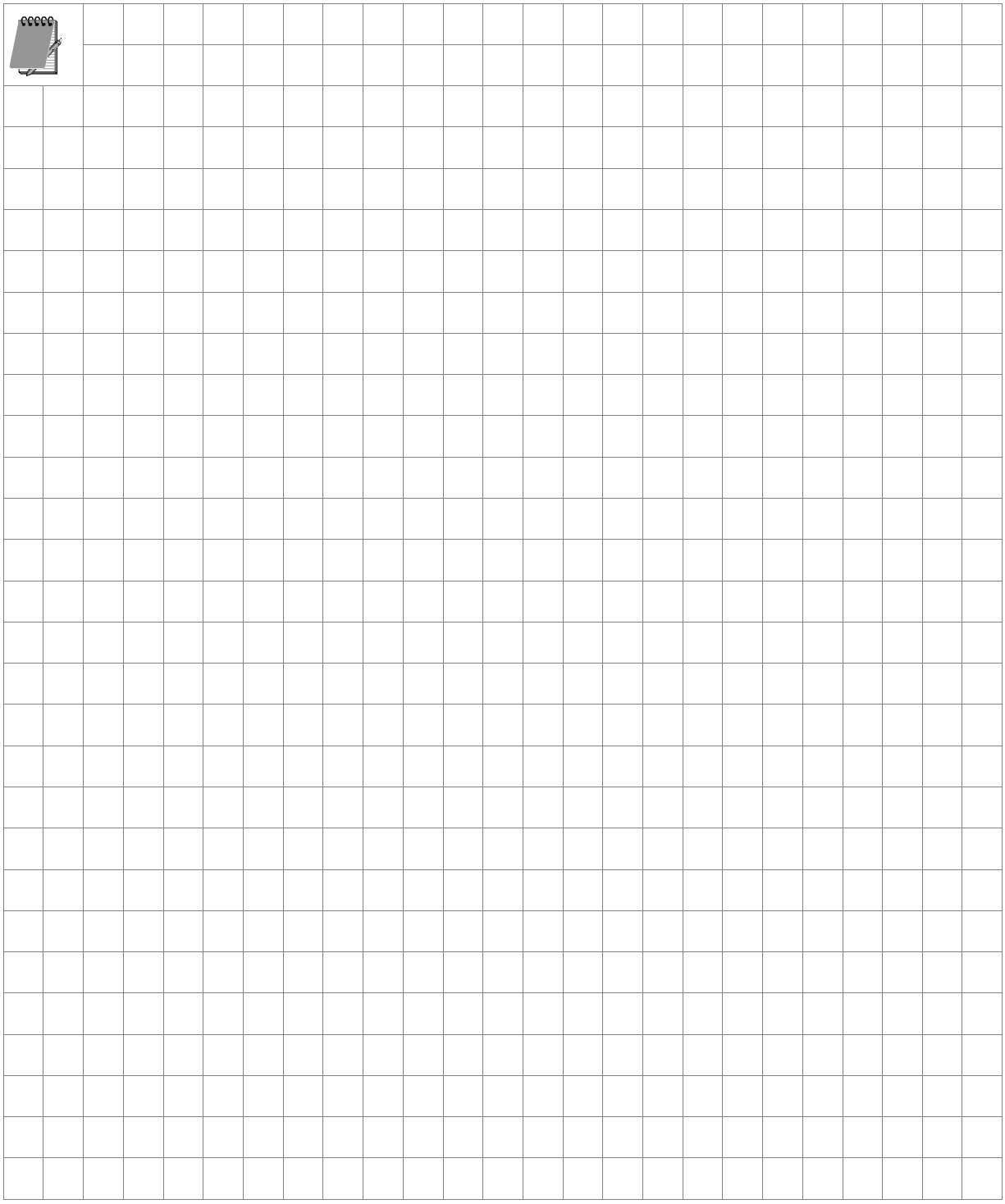


Abb.: Windows XP – Automatische Updates

Da die **Aktualisierung des Betriebssystems** Ihres PC in der Verantwortung des Administrators liegen muss und die Installation keinesfalls ohne ihn durchgeführt werden darf, ist diese Funktion durch den Administrator zu deaktivieren.



Anlagen

Checkliste für Datensicherheit am PC-Arbeitsplatz

- ☑ Sie haben sich das backUp-Magazin "PC-Arbeitsplatz" besorgt und überprüfen Ihren Arbeitsplatz-PC mithilfe dieser Checkliste.
- ☐ Sie sind in geeigneter Weise in der Benutzung Ihres Computers und Ihrer Fachanwendungen geschult und dabei auch über die grundsätzlichen Datensicherheitsmaßnahmen informiert worden.
- ☐ Ihnen sind Informationen über die Nutzung und Handhabung Ihres Computers und Ihrer Fachanwendungen an die Hand gegeben worden.
- ☐ PC, Monitore und Drucker dürfen nur vom Administrator umgestellt werden.
- ☐ Sie setzen keine private Hardware, Software und/oder Datenträger am Arbeitsplatz ein. Die private Nutzung von dienstlichen Datenträgern ist nicht gestattet.
- ☐ Sie verarbeiten nur die personenbezogenen Daten, die Sie für Ihr Aufgabengebiet benötigen.
- ☐ Sie verschließen Unterlagen mit personenbezogenen Daten in Aktenschränken.
- ☐ Beim Verlassen Ihres Büros schließen Sie entweder die Tür oder sperren den PC.
- ☐ Es sind kennwortgeschützte Bildschirmschoner installiert.
- ☐ Sie werfen keine Fehlkopien in den Papierkorb neben dem Kopierer.
- ☐ Sie verwalten Ihre Schlüssel sicher.

- ☐ Sie sorgen dafür, dass Unterlagen mit personenbezogenen Daten geschreddert werden.
- ☐ Sie stellen sicher, dass sich Benutzer nur in Ihrer Anwesenheit in Ihrem Büro befinden.
- ☐ Sie stellen sicher, dass der Bildschirm so ausgerichtet ist, dass kein Unbefugter Daten auf dem Bildschirm lesen kann.
- ☐ Sie können das IT-System nur nach Eingabe Ihrer Nutzerkennung (z. B. Organisationszeichen) und der Eingabe Ihres Passwortes benutzen.
- ☐ Es sind konkrete Regelungen für den Umgang mit Passwörtern hinsichtlich der Geheimhaltung, Mindestlänge und Gültigkeit sowie hinsichtlich der Überwachung des ordnungsgemäßen Umgangs getroffen worden.
- ☐ Sie wählen ein Passwort, das Zahlen, Buchstaben und Sonderzeichen enthält.
- ☐ Sie halten Ihr Passwort geheim, schreiben es nicht auf und ändern es regelmäßig.
- ☐ Sie geben Ihr Passwort an keine dritte Person weiter, auch nicht an den Administrator!
- ☐ Die Anzahl Ihrer Anmeldeversuche ist begrenzt. Nicht erfolgreiche Anmeldeversuche werden aufgezeichnet.
- ☐ Ihre Benutzeroberfläche ist an Ihr Aufgabengebiet angepasst worden.
- ☐ Die Funktionen von System- und Anwendungssoftware sind für Sie auf das zur Aufgabenerfüllung erforderliche Maß beschränkt.
- ☐ Der Administrator hat Ihnen eine gut strukturierte zentrale Ablage zur Verfügung gestellt.

- ☐ Sie besitzen einen *eigenen* Ordner in der zentralen Ablage, in dem Sie Ihre Dokumente ablegen können.
- ☐ Kollegen anderer Fachabteilungen haben keinen Zugriff auf Ihren Ordner.
- ☐ Werden Dokumente mit Microsoft Word erstellt, dann werden diese standardmäßig in einem zentralen Ordner auf dem Server gespeichert.
- ☐ Sie speichern keine Daten auf der lokalen Festplatte.
- ☐ Sie löschen automatisiert gespeicherte Dokumente, wenn sie nicht mehr erforderlich sind. Sie löschen sie spätestens mit Ablauf der Aufbewahrungsfristen, die für Akten gelten.
- ☐ Die Zugriffsberechtigungen der Benutzer werden vom Administrator auf Anweisung vergeben und von ihm dokumentiert.
- ☐ Das Disketten- und das CD-ROM-Laufwerk Ihres Arbeitsplatz-PC ist deaktiviert.
- ☐ USB-Speichermedien können nicht genutzt werden.
- ☐ Bei dienstlicher Erfordernis wird Ihr Disketten- und CD-ROM-Laufwerk vom Administrator für die Dauer der Maßnahme freigeschaltet.
- ☐ Eingehende Disketten geben Sie

  beim Administrator ab und lassen sie auf Viren prüfen.
- ☐ Datenträger, die Sie an Dritte weitergeben, haben Sie vor dem Beschreiben neu formatiert.
- ☐ Werden Datenträger ausgesondert oder vernichtet, werfen Sie sie nicht in den Papierkorb, sondern geben sie zur zentralen Vernichtung beim Administrator ab.
- ☐ Die Datenträger und Festplatten mobiler PC sind verschlüsselt.

- ☐ Die Verarbeitung personenbezogener Daten außerhalb der Organisation darf nur auf dienstlichen mobilen PC zu dienstlichen Zwecken erfolgen.
- ☐ Bei der Auswahl von Software werden zertifizierte Produkte bevorzugt.
- ☐ Soweit möglich wird Standardsoftware eingesetzt, Eigenentwicklungen sind nicht zulässig.
- ☐ Fachanwendungen, die Sie mithilfe von Standardsoftware wie ACCESS, EXCEL oder WORD erstellen, lassen Sie vom Fachvorgesetzten genehmigen.
- ☐ Die Nutzung des Internets ist auf die Dienste E-Mail und World Wide Web begrenzt.
- ☐ E-Mails, die personenbezogene Daten enthalten, versenden Sie grundsätzlich nur in verschlüsselter Form.
- ☐ Empfangene E-Mails löschen Sie nach Kenntnisnahme bzw. nach Ausdruck.
- ☐ In Ihrer Organisation wird ein Antivirenprogramm eingesetzt.
- ☐ Downloads und aktive Inhalte werden geblockt.

Muster einer Dienstanweisung für PC-Arbeitsplätze (Variante 1)

1. Vorbemerkungen

1.1 Zweck

Diese Dienstanweisung regelt die Nutzung von informationstechnischen Systemen (IT-Systeme) sowie die ordnungsgemäße Verarbeitung von Informationen im Hinblick auf die geltenden Bestimmungen des Datenschutzes sowie die gesetzlichen und betrieblichen Anforderungen an die Datensicherheit.

Durch den IT-Einsatz wird auch das Ziel verfolgt, die Arbeitsplatzqualität zu erhöhen, den Zeitaufwand für die Erledigung von Routineaufgaben zu verkürzen, die Arbeitsergebnisse zu steigern und den Austausch von Informationen - soweit erforderlich und zulässig - zu ermöglichen bzw. zu erleichtern.

Grundsätzlich wird Standardsoftware eingesetzt. Nur wenn keine für die Erledigung der Aufgaben geeignete Standardsoftware erhältlich ist, kommen Eigenentwicklungen in Betracht.

Die in dieser Dienstanweisung verwendeten Amts- und Funktionsbezeichnungen sowie die sonstigen personenbezogenen Bezeichnungen gelten für Frauen in der weiblichen und für Männer in der männlichen Sprachform.

1.2 Geltungsbereich

Die Dienstanweisung gilt für alle Arbeitsplätze mit IT-Unterstützung in der Organisation.

1.3 Rechtsgrundlagen

Die Möglichkeiten der unbefugten Einsichtnahme in vertrauliche Daten, der Datenzerstörung, des -diebstahls und der Verfälschung sind durch den Einsatz von IT-Systemen auf ein vertretbares Restrisiko zu reduzieren. Es ist daher ein disziplinierter und sorgfältiger Umgang mit den Funktionen der IT-Systeme geboten.

Zum Schutz personenbezogener Daten sind die bereichsspezifischen Gesetze sowie das geltende Datenschutzrecht zu beachten.

1.4 Begriffe

Unter IT-Unterstützung wird jede Hilfe bei der Verarbeitung und Übertragung von Informationen verstanden, zu der Geräte der Datenverarbeitung (Hardware) zusammen mit Programmen (Software) eingesetzt werden.

Datenschutz ist die Gewährleistung des informationellen Selbstbestimmungsrechts des Betroffenen bei der Verarbeitung personenbezogener Daten, d.h. der Einzelne ist davor zu schützen, dass er durch die Verarbeitung personenbezogener Daten in unzulässiger Weise in seinen Rechten beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen.

Datensicherheit ist die Gesamtheit der technischen und organisatorischen Maßnahmen, die eine störungsfreie und gegen Missbrauch gesicherte Datenverarbeitung zum Ziel haben. Die Sicherheit von Daten und Programmen ist insbesondere dadurch zu gewährleisten, dass

- der Zugriff auf Daten und Programme nur berechtigten Personen möglich ist,
- keine unberechtigte Nutzung oder Veränderung von gespeicherten Daten und Programmen erfolgt,
- Daten und Programme nicht verfälscht werden,
- die Verarbeitung der Daten und jede Veränderung der Programme dokumentiert wird und
- die Daten und Programme vor Verlust geschützt und reproduzierbar sind.

Unter dem Begriff Personal-Computer (PC) werden im Folgenden auch alle sonstigen Arbeitsplatzrechner (z. B. Macintosh-Rechner, UNIX-Workstations, Server-Arbeitsplätze, Terminals, Netz-Computer) verstanden. Die Regelungen dieser Dienstanweisung sind auf solche Geräte sinngemäß anzuwenden.

2. Zuständigkeiten und Verantwortungsbereiche

Die Verantwortung für die ordnungsgemäße Verarbeitung der Daten im Hinblick auf die Anforderungen des Datenschutzes und der Datensicherheit obliegt der Leitungsebene (Abteilungsleiter, Fachbereichsleiter etc.) in ihren Zuständigkeitsbereichen. Der jeweilige Leiter

sichert durch Organisation und Kontrolle die Einhaltung der Vorschriften seiner Mitarbeiter. Die o.g. Verantwortlichen werden im Folgenden als Leiter der Fachabteilungen bezeichnet.

2.1 Datenschutzbeauftragter der Organisation

Es ist ein Datenschutzbeauftragter bestellt. Er untersteht direkt dem Leiter der Organisation. Er ist bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Der Datenschutzbeauftragte informiert und berät die Mitarbeiter der Organisation in Datenschutzangelegenheiten und überwacht die Einhaltung der Datenschutzvorschriften. Die Aufgaben des Datenschutzbeauftragten sind in Anlage 1 aufgeführt.

2.2 Abteilung für Informations- und Kommunikationstechnik (IT-Abteilung)

Die IT-Abteilung ist eine zentrale Dienstleistungseinrichtung der Organisation für die Konzeption und Entwicklung sowie die betriebliche und technische Betreuung von Informations- und Kommunikationssystemen.

Die Anlage 2 gibt einen Überblick über die Aufgaben der IT-Abteilung. Bei der Erfüllung der Aufgaben arbeitet sie eng mit den Leitern der Fachabteilungen bzw. mit den dort tätigen IT-Beauftragten zusammen.

2.3 IT-Beauftragte

Die Leiter der Fachabteilungen bestimmen für ihren Verantwortungsbereich einen fachlich geeigneten IT-Beauftragten, der als Betreuer für IT-Anwendungen tätig ist. Dabei ist eine Vertretung sicherzustellen. Die IT-Beauftragten sorgen in ihrem Zuständigkeitsbereich dafür, dass die Anforderungen des Datenschutzes und der Datensicherheit durch geeignete und angemessene Maßnahmen gewährleistet werden, überwachen die Datenverarbeitung und betreuen die IT-Anwender. Die IT-Beauftragten nehmen die IT-Probleme der Nutzer auf und bearbeiten sie - ggf. mit Unterstützung durch die IT-Abteilung. Sie sind der Ansprechpartner der IT-Abteilung. In Fragen des Datenschutzes arbeiten die IT-Beauftragten eng mit dem Datenschutzbeauftragten der Organisation zusammen. Die Aufgaben der IT-Beauftragten sind der Anlage 3 zu entnehmen.

2.4 IT-Nutzer

Dem IT-Nutzer obliegen vor allem

- die Verantwortung für die Ordnungsmäßigkeit des Arbeitsablaufes,
- die Sicherstellung der datenschutzrechtlichen Zulässigkeit der Verarbeitung personenbezogener Daten,
- die Verantwortung, nur freigegebene und aktuell gültige Programme einzusetzen,
- die regelmäßige Erstellung von Sicherungskopien der Daten und ggf. Programme, soweit kein anderes Verfahren vorgesehen ist,
- der Schutz der IT-Systeme vor unbefugter, unsachgemäßer und missbräuchlicher Benutzung und
- die Pflege der IT-Systeme.

Bei Fragen und Problemen wendet sich der IT-Nutzer an den für ihn zuständigen IT-Beauftragten, dem auch unerwartetes Systemverhalten, ungewöhnliche Ereignisse sowie jeder Datenverlust mit unbekannter Ursache unverzüglich zu melden sind.

3. Benutzungsbestimmungen

Die nachfolgenden Anleitungen gelten für die Nutzung von IT zur Lösung arbeitsplatzbezogener Fachaufgaben.

3.1 Grundsätze

- Vor dem erstmaligen IT-Einsatz ist eine ausreichende Schulung der Benutzer unter Berücksichtigung der datenschutzrechtlichen Anforderungen zu gewährleisten.
- Es dürfen nur dokumentierte, für den jeweiligen Arbeitsplatz freigegebene und aktuell gültige Programme eingesetzt werden.
- Das Einspielen und die Nutzung von nicht ordnungsgemäß lizenzierter oder privat beschaffter Software ist nicht zulässig.

- Soweit in Lizenzverträgen die private Mitbenutzung dienstlich beschaffter Software gestattet ist, sind die jeweiligen Bestimmungen zu beachten.
- Die zur Verfügung gestellte Hard- und Software darf nur für dienstliche Aufgaben im Rahmen des Nutzungskonzeptes eingesetzt werden. Änderungen und Erweiterungen an der Hardware dürfen nur von der IT-Abteilung vorgenommen werden.
- Die Nutzung privater IT-Systeme ist grundsätzlich unzulässig.
- Personenbezogene Daten dürfen nur im zugelassenen Rahmen verarbeitet werden.
- Grundsätzlich dürfen für Testzwecke nur Testdaten oder anonymisierte Echtdaten verwendet werden.
- Die dienstliche Nutzung privater Daten und die private Nutzung dienstlicher Daten sind nicht zulässig.
- Jede Weitergabe von Programmen und Daten an Dritte ist nur im Rahmen der gesetzlichen Vorschriften und Lizenzbedingungen sowie nach ausdrücklicher Genehmigung des Leiters gestattet.
- Der Aufbau benutzereigener Verfahren ist nur im Einvernehmen mit der IT-Abteilung zugelassen. Die Verfahren sind so zu dokumentieren, dass ein sachverständiger Dritter in angemessener Zeit die Nutzung und Pflege der Programme übernehmen kann.
- Die Installation der System- und Anwendungssoftware und jede Veränderung ist von der IT-Abteilung durchzuführen.

3.2 Zugangs – und Zugriffsberechtigungen

- Zu Räumen, in denen IT-Systeme installiert sind, dürfen nur Berechtigte Zugang haben. Außenstehende, zu denen auch das Wartungspersonal von Fremdfirmen gehört, dürfen sich nur in Begleitung eines Mitarbeiters der Abteilung in diesen Räumen aufhalten.
- Sofern keine speziellen Zugangskontrollen vorhanden sind, sind unbesetzte Räume mit IT-Systemen abzuschließen. Die Schlüssel sind so aufzubewahren, dass sie nicht von Unbefugten benutzt werden können.

- Bei der Verarbeitung von personenbezogenen Daten ist zu verhindern, dass Unbefugte Einblick in die laufende Datenverarbeitung haben. Insbesondere bei Stellen mit Publikumsverkehr muss der Monitor so aufgestellt werden, dass Unbefugte diesen nicht einsehen können.
- Diejenigen Personen, die zur Nutzung von zentralen IT-Verfahren berechtigt sind, sind vom IT-Beauftragten auf der Basis eines Berechtigungskonzeptes der IT-Abteilung zu benennen. Die Berechtigung darf sich lediglich auf die für die Aufgabenerfüllung erforderlichen Anwendungen erstrecken.
- Alle für den Arbeitsplatz eingerichteten, servergestützten Anwenderfunktionen dürfen nur nach Eingabe einer Benutzerkennung, gekoppelt mit nachfolgender Passworteingabe, aktiviert werden. Näheres ist der Anlage 4 zu entnehmen.

3.3 Arbeitsablauf

- Alle Daten sind zentral in den dafür vorgesehenen Ablagen zu speichern. Auf den lokalen Festplatten sind keine Daten abzulegen.
- Sofern schützenswerte Informationen verarbeitet werden und Dritte Zugang zum Arbeitsplatz haben können, sind Bildschirmschoner so einzustellen, dass bei Arbeitsunterbrechung nach einem Zeitintervall von max. 10 Minuten auf Bildschirmdunkelschaltung mit Passwortaktivierung umgeschaltet wird. Beim Verlassen des Arbeitsplatzes muss die Bildschirmdunkelschaltung mit Passwortaktivierung (Anlage 4) am PC manuell eingeschaltet werden.
- Bei servergestützten Anwendungen ist der Dialog bei längerer Abwesenheit abzumelden, sofern dies nicht automatisch erfolgt.
- Bei Dienstende sind die aktivierten Programme ordnungsgemäß zu beenden und - soweit keine andere dienstliche Regelung besteht - der PC auszuschalten.
- Nach Abschluss der Arbeiten sind alle Ausdrucke aus dem Drucker zu entfernen.
- Drucker sind so aufzustellen, dass nur Berechtigte Zugang haben.

3.4 Handhabung und Verwaltung von Datenträgern

- Datenträger sind mit Klebeetiketten eindeutig zu kennzeichnen. Die Beschriftung soll für interne Zwecke die Einrichtung, den Bearbeiter, den Inhalt und das Erstellungsdatum aufweisen. Beim Versand von Datenträgern darf die Beschriftung jedoch für Unbefugte keine Rückschlüsse auf den Inhalt des Datenträgers erlauben.
- Besonders sensible Daten sind zu verschlüsseln.
- Auf Datenträgern, die schützenswerte, nicht mehr benötigte Daten speichern, ist vor Wiederverwendung die Löschung der gespeicherten Daten durch vollständiges Überschreiben oder Formatieren vorzunehmen.
- Die Datenträger sind magnetfeld- und staubgeschützt in speziellen Boxen und in abschließbaren Schränken aufzubewahren, so dass sie vor unbefugtem Zugriff geschützt sind.
- Beim Versand von Datenträgern ist sicherzustellen, dass der Empfänger nur die für ihn bestimmten Daten erhält.
- Fachabteilungen, die einen Datenträgeraustausch durchführen, müssen einen Datenträgernachweis (z. B. systematische Ablage der "Begleitscheine für Datenträger") führen. Zu- und Abgänge sind mit Angabe der übergebenden bzw. übernehmenden Person, zum Datenträgerinhalt und zum Anlass des Transports zu vermerken.
- Das Einspielen von Datenträgern ist vom IT-Beauftragten zu koordinieren.

3.5 Entsorgung von IT-Systemen und Datenträgern

- Defekte oder nicht mehr benötigte IT-Systeme und Festplattenspeicher dürfen nur der IT-Abteilung zur kontrollierten Weiterverwendung oder Vernichtung überlassen werden.
- Disketten, Magnetbänder, Magnetbandkassetten, CD-ROMs etc., die nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind von der nutzenden Stelle durch physikalische Löschung bzw. mechanisch so zu zerstören, dass keine Rückschlüsse auf vorher gespeicherte Daten mehr möglich sind.

- Die gelöschten bzw. zerstörten Datenträger werden beim IT-Beauftragten zur umweltgerechten Entsorgung übergeben.

Datum ……

Leiter der Organisation

Aufgaben des Datenschutzbeauftragen (Anlage 1)

(Kurzbeschreibung)

- Überwachung der Einhaltung der geltenden Datenschutzbestimmungen.
- Regelmäßige Information und Schulung der Mitarbeiter der Organisation in Fragen des Datenschutzes.
- Überwachung des ordnungsgemäßen Einsatzes der IT-Systeme, mit denen personenbezogene Daten verarbeitet werden.
- Beratung der Abteilungsleiter bei Grundsatzfragen und schwierigen Einzelfragen des Datenschutzes.
- Beratung und Unterstützung der IT-Abteilung und der IT-Beauftragten.
- Erarbeitung und Fortschreibung eines Datenschutzkonzeptes.

Aufgaben der IT-Abteilung (Anlage 2)

(Kurzbeschreibung)

- Erarbeitung und Fortschreibung eines Rahmenkonzepts für die Informations- und Kommunikationstechnik.
- Aufbau und Fortentwicklung der Infrastruktur für ein umfassendes Informations- und Kommunikations-System (Hardware, Software, Netz).

- Bereitstellung, Betrieb und Überwachung der zentralen Server und des Kommunikationsnetzes sowie Sicherung des Netzes gegen unbefugte Zugriffe von außen (Firewall).
- Administration, Routineeinsatz und Datensicherung der zentralen IT-Verfahren und Datenbanken.
- Konzeption von DV-Verfahren, Programmentwicklung bzw. -übernahme, Programmanpassung und -pflege sowie Verfahrensdokumentation.
- Aufbau und Pflege zentraler Informationsdienste.
- Beschaffung von Hard- und Software sowie von Netzkomponenten.
- Installation von Hard- und Software sowie Einweisung in die sachgerechte Handhabung der Systeme, soweit dies nicht von den IT-Beauftragten durchgeführt werden kann.
- Organisation und Durchführung von Maßnahmen zur Aus- und Fortbildung im Bereich der Informations- und Kommunikationstechnik.
- Instandsetzung der IT-Anlagen, IT-Systeme und Netzkomponenten.
- Unterstützung der IT-Beauftragten in Fragen des Datenschutzes und der Datensicherheit sowie bei DV-technischen Problemen (Second Level Support).
- Führung eines Hard- und Software-Registers mit allen IT-Systemen und Programmen der Organisation.
- Zusammenarbeit mit dem Datenschutzbeauftragten in Bezug auf die Planung, Entwicklung und Einführung von IT-Verfahren, mit denen personenbezogene Daten verarbeitet werden sollen.

Aufgaben der IT-Beauftragten (Anlage 3)

(Kurzbeschreibung)

- Einrichtung und Verwaltung von Benutzerkennungen und Zugriffsrechten innerhalb der Fachverfahren sowie Erstzuweisung von Passwörtern und Kontrolle eines regelmäßigen Passwortwechsels.

- Konzeption, Überwachung und ggf. Durchführung von Maßnahmen zur Sicherung von Daten und Programmen in Absprache mit der IT-Abteilung.
- Kontrolle der Installation und der Aktualisierung von Software auf den PC-Arbeitsplätzen sowie des Zugangsschutzes zu den Systemen.
- Umsetzung der Bestimmungen für die Benutzung der IT-Systeme und Erstellung von Arbeitsanleitungen.
- Überprüfung der an den einzelnen Arbeitsplätzen eingesetzten Software auf ihre Zulässigkeit.
- Behebung von Störungen (First Level Support).
- Wiederherstellung von Daten und Programmen nach Fehlern und Störungen.
- Beratung und Unterstützung der IT-Nutzer.
- Erarbeitung von Vorschlägen für die Verbesserung und Weiterentwicklung der IT-Anwendungen.
- Planung des Hard- und Software- sowie des Schulungsbedarfs.
- Rechtzeitige Information des Datenschutzbeauftragten über die Planung, Entwicklung und Einführung von IT-Verfahren, mit denen personenbezogene Daten verarbeitet werden sollen.

Passwort-Schutz (Anlage 4)

Umgang mit Passwörtern

- Auf jedem PC ist ein BIOS-Passwort sowie ggf. ein Bildschirmschoner mit Passwortaktivierung einzurichten.
- Bei servergestützten Anwendungen wird dem Benutzer auf der Grundlage eines Berechtigungskonzeptes für die vorgesehene Funktion vor der erstmaligen Nutzung vom IT-Beauftragten bzw. von der IT-Abteilung eine Benutzerkennung und ein Initialpasswort eingerichtet und persönlich mitgeteilt.

- Beim erstmaligen Anmelden an einer Server-Anwendung ist das Initialpasswort durch ein persönliches Passwort zu ersetzen. Es darf keine Rückschlüsse auf seinen Besitzer zulassen und ist vertraulich zu behandeln.
- Die IT-Abteilung verwahrt die für den Betrieb wichtigen Passwörter (z. B. für BIOS und Systemverwalterkennung).
- Besteht der Verdacht, dass Unbefugte Kenntnis von einem Passwort erhalten haben, ist unverzüglich ein neues Passwort einzurichten. Darüber hinaus ist das Passwort in unregelmäßigen Zeitabständen - spätestens jedoch nach 3 Monaten - zu ändern, sofern das System nicht automatisch dazu auffordert.
- Passwörter dürfen nicht unverschlüsselt in Dateien abgelegt werden.
- Programmierbare Tasten sollten niemals mit den Zugangsdaten (Benutzerkennung, Passwort) oder sonstigen sicherheitsrelevanten Daten belegt werden.
- Sämtliche schriftlichen Unterlagen, aus denen Rückschlüsse auf Zugangsmöglichkeiten zum System (z. B. Benutzerkennung, Passwort) gezogen werden können, sind sorgfältig und für Unbefugte unzugänglich aufzubewahren.

Hinweise für die Wahl eines guten Passwortes

Bei der Auswahl eines Passwortes sollte darauf geachtet werden, dass es nicht leicht erratbar ist. Problematisch sind alle Passwörter, die von einem Angreifer ausprobiert werden können, z. B.:

- Trivialkennwörter wie "ABC" oder Tastaturfolgen (z. B. "qwert" oder "asdfgh"),
- Worte aus dem Sprachschatz,
- Worte aus anderen Sprachen,
- alle Arten von Namen (Personen, Städte, Gebäude, Comic-Figuren, ...),
- persönliche Namen, die Namen von Familienangehörigen, Haustieren, Automarken und Autokennzeichen,
- Rechnernamen, Benutzerkennungen oder Teile davon,

- Geburtsdaten, Telefonnummern,
- Abkürzungen,
- Anhängen oder Voranstellen einer Zahl oder eines anderen Zeichens (peter09, 7peter,peter$, %peter, ...),
- Rückwärtsschreiben (retep, reteP,...).

Damit ein Kennwort nicht durch die vollständige Suche (d.h. automatisiertes Ausprobieren aller möglichen Kombinationen) ermittelt werden kann, sollte ein Passwort mindestens 6 Zeichen lang sein und möglichst immer aus einer Kombination von Buchstaben, Ziffern und Sonderzeichen bestehen.

Ein gutes Passwort ist z. B. nd2@6e$f (aber bitte nicht benutzen!!)

Muster einer Dienstanweisung für PC-Arbeitsplätze (Variante 2)

1. Vorbemerkung

Diese Dienstanweisung soll unter Berücksichtigung des Sicherheitskonzepts eine nach einheitlichen Grundsätzen gestaltete, sichere und ordnungsgemäße Datenverarbeitung gewährleisten.

Sie findet Anwendung auf

- alle technischen Systeme und Verfahrensabläufe, mit deren Hilfe dienstliche Informationen gespeichert und weiterverarbeitet werden können,
- personenbezogene Daten, die mithilfe der zuvor genannten Systeme elektronisch verarbeitet werden und
- personenbezogene Daten, die in herkömmlichen Akten verarbeitet werden.

Diese Dienstanweisung gilt für alle Mitarbeiter der Organisation, die für die Erledigung ihrer Aufgaben elektronische Datenverarbeitungssysteme nutzen, und/oder im Rahmen ihrer Aufgabenwahrnehmung personenbezogene Daten verarbeiten.

2. Benutzung der Hardware

- Lassen Sie sich von Ihrem Administrator vor der erstmaligen Benutzung (neuer) Datenverarbeitungssysteme und Verfahren zunächst schulen und sich auch über die grundsätzlichen Datensicherheitsmaßnahmen informieren.
- Überzeugen Sie sich von der vollständigen und sachgerechten Ausgestaltung Ihres Arbeitsplatzes. Hierzu gehört insbesondere die funktionsgerechte Aufstellung der Geräte und die Blendfreiheit bei Datensichtgeräten. Die Monitore sollten quer zum einfallenden Licht und zur Schonung der Augen in einem ausreichenden Abstand aufgestellt werden (je nach Bildschirmgröße 55 bis 80 cm).

- Achten Sie gemeinsam mit dem Administrator darauf, dass die Geräte darüber hinaus so an Ihrem Arbeitsplatz platziert werden, dass eine unbefugte Kenntnisnahme von dargestellten oder ausgedruckten Informationen (z. B. durch Besucher oder sonstige Nichtbeteiligte) ausgeschlossen ist.
- Lassen Sie sich von Ihrem Administrator geeignetes Material über die Nutzung und Handhabung „Ihres PC“ geben (Benutzerhandbuch, Bedienungsanweisungen). Die in den Bedienungsanweisungen festgelegten Regelungen sind zu beachten. Da die Anweisungen zum jeweiligen Gerät gehören, lassen Sie sie bitte bei einem Arbeitsplatzwechsel an Ihrem bisherigen Arbeitsplatz zurück.
- Behandeln Sie ihren PC „pfleglich“. Bitte versuchen Sie bei technischen Störungen nicht, diese selbst zu beheben, indem Sie das Gerät öffnen oder technisch verändern. Informieren Sie stattdessen Ihren Administrator.
- PC, Monitore und Drucker dürfen nur vom Administrator nach vorheriger Registrierung im Geräteverzeichnis entfernt und umgestellt werden.
- Der Einsatz privater Hardware am Arbeitsplatz ist unzulässig.
- Der Administrator ist für den ordnungsgemäßen Betrieb und die Betreuung der EDV-Systeme sowie die Umsetzung der technischen Datensicherheitsmaßnahmen zuständig.
- Lassen Sie Ihren PC nicht ohne Aufsicht in unverschlossenen, frei zugänglichen Räumen stehen.
- Nutzen Sie stets den vom System angebotenen kennwortgeschützten Bildschirmschoner. Dieser stellt einen wirksamen Schutz gegen unbefugte Kenntnisnahmeversuche dar, insbesondere dann, wenn Sie Publikumsverkehr haben. Bei längerer Arbeitsunterbrechung ist der PC nach ordnungsgemäßer Abmeldung auszuschalten.
- Ihr Passwort ist Ihr „persönlicher Schlüssel“ zu Ihrem PC. Sorgen Sie dafür, dass ihn kein anderer benutzen kann und dass er Ihnen nicht abhanden kommt.
- Konkrete Hinweise für den Umgang mit Passworten hinsichtlich der Geheimhaltung, Mindestlänge und Gültigkeit erhalten Sie von Ihrem Administrator.

3. Einsatz und Nutzung von elektronischen Datenträgern (Disketten, CD-ROM)

- Der Einsatz privater Datenträger am Arbeitsplatz ist nicht gestattet.
- Die private Nutzung von dienstlichen Datenträgern ist ebenfalls nicht gestattet.
- Sollten Sie im Rahmen Ihrer Aufgabenerledigung Disketten von externen Stellen erhalten, geben Sie diese immer zunächst bei Ihrem Administrator ab, damit sie dort auf Viren geprüft werden können.
- Wenn Sie mit Zustimmung Ihres Fachdienst-/Amtsleiters Datenträger an Dritte weitergeben, formatieren Sie diese zunächst neu und registrieren Sie sie in einem Nachweis mit Ausgangsdatum und Empfänger. Bitte vermerken Sie darin auch den Zeitpunkt und die Art der Rückgabe.
- Datenträger sind zum Schutz gegen Diebstahl in verschlossenen Behältnissen aufzubewahren (z. B. Schrank oder Schreibtisch).
- Geben Sie ausgesonderte Datenträger immer bei Ihrem Administrator zur Vernichtung ab. Diese werden dort fachgerecht so entsorgt, dass der Inhalt, also die Daten, nicht mehr erkennbar gemacht werden können.

4. Nutzung mobiler PC

- Falls Sie im Rahmen Ihrer Aufgabenwahrnehmung personenbezogene Daten außerhalb der Organisation (z. B. im Außendienst oder bei Hausbesuchen) verarbeiten, darf dies nur auf dienstlichen Geräten und zu dienstlichen Zwecken erfolgen.
- Mobile PC sind nach Dienstschluss im Büro unter Verschluss zu halten.
- Soweit Ihnen Ihr Fachdienst-/Amtsleiter die Mitnahme Ihres dienstlichen mobilen PC nach Hause gestattet hat, nehmen Sie das Gerät bitte auch dort unter Verschluss.
- Stellen Sie sicher, dass bei Ihrem mobilen PC die Option „Passwortschutz“ aktiviert ist, und vergeben Sie sich ein sicheres Passwort.
- Hinterlegen Sie dieses Passwort im verschlossenen Umschlag bei Ihrem Amts- oder Fachdienstleiter.

- Mobile PC, auf denen personenbezogene Daten verarbeitet werden, sind zwingend mit Sicherheitssoftware auszustatten, die insbesondere die Möglichkeit bietet, personenbezogene Daten verschlüsselt zu speichern. Die erforderliche Sicherheitssoftware wird Ihr Administrator für Sie installieren.

5. Nutzung und Entwicklung von Software

- Die private Nutzung von dienstlicher Software für private Zwecke ist unzulässig.
- Dienstlich beschaffte Programme dürfen nicht kopiert werden.
- Eigenentwicklungen außerhalb von Standardsoftware wie Access, Excel oder Word sind nicht zulässig, weil der Dokumentations- und Pflegeaufwand hierfür zu groß ist.
- Wenn Sie Anwendungen mithilfe von Standardsoftware erstellen, benötigen Sie hierfür zunächst die Genehmigung Ihres Fachdienst-/Amtsleiters, da dieser die Verantwortung für die Zulässigkeit der Datenverarbeitung trägt.

6. Datenhaltung

- Bei allen vernetzten Geräten sind die Datenbestände zentral auf dem jeweiligen Server zu speichern. Eine lokale Speicherung auf einer vernetzten Arbeitsstation ist damit grundsätzlich nicht erforderlich und nur im Ausnahmefall mit Zustimmung des Fachdienstleiters zulässig.
- Das Kopieren von dienstlichen Datenbeständen für private Zwecke ist unzulässig.
- Löschen Sie automatisiert gespeicherte Dokumente mit personenbezogenen Daten, wenn sie nicht mehr erforderlich sind. Dies ist regelmäßig dann der Fall, wenn Sie ein papierenes Verfügungsexemplar zur Akte genommen haben und das Originaldokument verschickt wurde.
- Im übrigen sind automatisiert gespeicherte Daten spätestens mit Ablauf der Aufbewahrungsfristen für Akten zu löschen.
- „Musterschreiben“, die Sie immer wieder verwenden, speichern sie bitte ohne personenbezogenen Inhalt.

7. Regelungen für Akten und nicht automatisierte Dateien (Karteien, Register)

- Die Zulässigkeit der Verarbeitung personenbezogener Daten in Akten richtet sich zunächst nach den bereichsspezifischen Datenschutzbestimmungen. Soweit entsprechende Regelungen fehlen, gelten die allgemeinen Bestimmungen des Landesdatenschutzgesetzes.
- Nicht besetzte Büroräume sind grundsätzlich zu verschließen.
- Der Schlüssel ist abzuziehen und sicher zu verwahren (persönlicher Gewahrsam oder Schlüsselschrank).
- Ist dies aus dienstlichen Gründen nicht möglich (z. B. weil Kollegen Zugriff auf die dort vorhandenen Unterlagen – z. B. Pläne oder Gesetzestexte - haben müssen), halten Sie die Unterlagen mit personenbezogenem Inhalt bei Abwesenheit unter Verschluss (Schrank, Schreibtisch) und verwahren Sie die Schlüssel ebenfalls sicher.
- Versenden Sie Akten mit personenbezogenen Daten, die einem besonderen Amtsgeheimnis unterliegen (z. B. Personaldaten, Sozialdaten oder Gesundheitsdaten), im internen Postgang oder an andere öffentliche Stellen (z. B. Gerichte) nur im verschlossenen Umschlag o. ä..
- Falls Sie im Rahmen Ihrer Aufgabenwahrnehmung personenbezogene Daten in Akten außerhalb der Organisation bearbeiten (z. B. im Außendienst oder bei Hausbesuchen), sind diese gegen unbefugte Zugriffe zu schützen. Das heißt, die Akte darf nicht unbeaufsichtigt aus der Hand gegeben werden. Sie ist z. B. im Auto nicht sichtbar unter Verschluss zu halten. Sie ist nach Dienstschluss grundsätzlich wieder ins Büro zurückzubringen. Wenn dies nicht möglich ist, ist sie zu Hause unter Verschluss zu nehmen.
- Papiergut mit personenbezogenem Inhalt muss datenschutzgerecht entsorgt werden. Entsorgen Sie Unterlagen mit personenbezogenen Daten, insbesondere Personal-, Sozial- oder Gesundheitsdaten, über den Etagenschredder.
- Personenbezogene Daten in Akten sind zu löschen, wenn ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Maßgeblich sind hier die bereichsspezifischen Aufbewahrungsfristen.

- Stellen Sie sicher, dass sich Besucher nur in Ihrem oder im Beisein eines anderen Mitarbeiters im Büro aufhalten.

Datum ……

Leiter der Organisation

Muster einer Dienstanweisung zur Nutzung der Internet-Dienste

1. Begriffsbestimmungen

- Das Internet ist ein weltweites Computernetzwerk, mit dessen Hilfe Daten ausgetauscht und Informationen veröffentlicht oder abgerufen werden. Die Inhalte unterliegen keinerlei Kontrolle hinsichtlich Art, Form und Inhalt. Somit resultiert aus jeder Nutzung dieses Mediums eine potenzielle Gefahr im Hinblick auf Datenschutz und Datensicherheit. Es können beispielsweise durch die uneingeschränkte Verbreitung von Programmen Computerviren oder Verfahren zum unberechtigten Ausspionieren oder Manipulieren von Daten in die an das Internet angeschlossenen Rechner eingeschleust werden.
- Die Internet-Technologie stellt den an das Internet angeschlossenen Rechnern verschiedene Dienste zur Verfügung. Der bekannteste Dienst ist das World Wide Web (WWW), das weltweit Informationen bereitstellt. Weiterhin basieren auf der Internet-Technologie die elektronische Post (E-Mail) sowie der Dateitransfer (FTP), mit dem größere Dateien über das Internet übertragen werden können.
- Der Begriff Intranet bezeichnet ein in sich geschlossenes internes Netzwerk, an das alle Rechner einer Organisation angeschlossen sind.
- Aus Sicherheitsgründen und zum Schutze vor unberechtigten Zugriffen aus dem Internet ins Intranet existiert nur eine fest definierte Schnittstelle zwischen den beiden Netzen. Sie ist durch spezielle Maßnahmen gesichert (Firewall, Virenscanner etc.).

2. Grundlage

Grundlagen für diese Dienstanweisung sind die bereichsspezifischen Gesetze, das Landesdatenschutzgesetz und die dazu erlassene Verordnung.

3. Geltungsbereich und Verantwortlichkeit

- Diese Dienstanweisung regelt die Nutzung der Internet-Dienste für alle PC-Benutzer/innen.

- Die technische Administration und Überwachung der Internetnutzung und der Netzwerksicherheit liegen beim Fachbereich Inneres.
- Die Fachdienstleiter sind für die organisatorische Umsetzung der in dieser Dienstanweisung getroffenen Regelungen zuständig.

4. Nutzung der Internet-Dienste

- Die Nutzung der Internet-Dienste erfordert von allen Mitarbeiterinnen und Mitarbeitern eine erhöhte Sensibilität auf Grund des hohen Vertraulichkeitsgrades der im PC-Netz der Organisation gespeicherten Daten.
- Das Internet dient als Informationsmedium für dienstliche Belange. Eine private Nutzung der Internetdienste ist unzulässig.
- Über das Intranet der Organisation stehen nur bestimmte Internet-Dienste zur Verfügung. Der Zugriff ist auf WWW und E-Mail beschränkt. Über eine Ausweitung auf andere Dienste entscheidet der Fachbereich Inneres auf Antrag in Abstimmung mit den betroffenen Fachdiensten.
- E-Mail-Eingänge sind wie allgemeine Posteingänge zu behandeln. Vorgangsbezogene E-Mails sind auszudrucken, dem Aktenvorgang zuzuordnen und anschließend zu löschen. Bei wichtigen Angelegenheiten sind E-Mail-Eingänge an die Vorgesetzte bzw. den Vorgesetzten weiterzuleiten.
- Alle Mitarbeiter/innen müssen täglich ihr elektronisches Postfach sichten und im Falle einer länger als einen Arbeitstag dauernden Abwesenheit für eine Umleitung der E-Mail-Eingänge Sorge tragen. Das gilt auch für die Vertreterin oder den Vertreter, bei Krankheit oder sonstiger unvorhergesehener Abwesenheit der Mitarbeiterin oder des Mitarbeiters.
- Der Zugriff auf WWW ist auf bestimmte freigegebene Seiten beschränkt. Web-Seiten, die von dienstlichem Interesse sind, können auf Antrag durch die Fachdienste vom Fachbereich Inneres freigeschaltet werden. Eine Freigabe erfolgt nicht, wenn von der Seite ein erhöhtes Sicherheitsrisiko ausgeht (Die Möglichkeit, Programme mit schädigender Wirkung von einer Web-Seite herunterladen zu können, stellt bereits ein solches Gefährdungspotenzial dar!).

- In begründeten Ausnahmefällen kann ein nicht an das PC-Netz der Organisation angeschlossener Rechner vom Fachbereich Inneres zur Verfügung gestellt werden, über den ein voller Internet-Zugriff zum ausschließlichen Zwecke der Informationsrecherche möglich ist. Die Entscheidung trifft der Fachbereich Inneres. Mit diesem PC dürfen keine personenbezogenen Daten verarbeitet oder übermittelt werden. Personenbezogene Daten sind beispielsweise Name, Vorname und Anschrift einer Person, Gesundheits- und Arztdaten, Steuer- und Sozialdaten und Daten über strafbare Handlungen oder Ordnungswidrigkeiten. Die Einrichtung und Verwendung von E-Mail-Diensten ist an diesen PCs nicht gestattet.
- Die Nutzung der Internet-Dienste ist nur zulässig mit den Programmen, die vom Fachbereich Inneres für diesen Zweck konfiguriert und zur Verfügung gestellt werden.

5. Datenschutz und Datensicherheit

- Im Internet sind keinerlei organisatorische Maßnahmen zum Datenschutz und zur Datensicherheit getroffen. Der Fachbereich Inneres stellt deshalb sicher, dass an der Schnittstelle zwischen Internet und Intranet Maßnahmen zum Schutz vor Gefährdungspotenzialen wie Viren, Datenmanipulation und -zerstörung, Einschleusen von Trojanern etc. durch Einsatz einer Firewall und eines Virenscanners getroffen werden.
- Die Schnittstelle ins Internet wird vom Fachbereich Inneres zur Verfügung gestellt. Sie ist der einzige Übergang zwischen Intranet und Internet.
- Personenbezogene Daten dürfen grundsätzlich nur in verschlüsselter Form in das Internet übertragen werden.
- Sollte eine Verschlüsselung nicht möglich sein, weil ein Kommunikationspartner beispielsweise kein geeignetes Verfahren einsetzt, ist die Übertragung von personenbezogenen Daten mithilfe des Internet unzulässig. Als Alternative steht dann der Postweg zur Verfügung. Das Gleiche gilt für sonstige vertrauliche Daten (z. B. interne Richtlinien, Protokolle vertraulicher Besprechungen).

- Der Fachbereich Inneres stellt an einem IT-Arbeitsplatz ein geeignetes Verschlüsselungsverfahren zur Verfügung. Die öffentlichen Schlüssel von Kommunikationspartnern werden vom Fachbereich Inneres im Auftrag der Fachdienste signiert und zentral verwaltet.
- An jedem Arbeitsplatzrechner ist eine geeignete Virenerkennungssoftware zu installieren, die regelmäßig auf den neuesten Stand aktualisiert wird. Die Fachdienste stellen in Zusammenarbeit mit dem Fachbereich Inneres sicher, dass die Mitarbeiter/innen der Organisation im Umgang mit dem Werkzeug geschult werden.
- Solange die digitale Signatur (elektronische Unterschrift) in der Organisation nicht eingesetzt wird, kann der Inhalt einer E-Mail keine rechtsverbindliche Wirkung herbeiführen, die beispielsweise bei einer Kündigung oder einem Verwaltungsakt erforderlich ist. Als Alternative steht der Postweg zur Verfügung, in bestimmten Fällen auch Telefax.
- Das Herunterladen von Dateien ist unzulässig. Dienstlich notwendige Downloads werden vom Fachbereich Inneres auf Antrag durchgeführt. Heruntergeladene Dateien werden vor Benutzung auf Virenbefall geprüft.
- E-Mails mit Anhängen [Attachments] können nur verschickt und empfangen werden mit Anhängen der Typen:
  - Text-Dokumente (*.doc, *.rtf, *.wri, *.txt)
  - Excel-Arbeitsmappen (*.xls)
  - Präsentationen (*.ppt)
  - Grafiken (*.gif, *.jpg, *.tif, *.bmp, *.cdr)
  - Austauschformate (*.pdf)

- Der Fachbereich Inneres entscheidet auf Antrag der Fachdienste über die Aufnahme zusätzlicher Dateiformate.
- Alle E-Mails mit nicht zugelassenen Anhängen (z. B.: *.exe, *.com und *.vbs) werden in ein separates zentrales Fach der administrativen Ebene umgeleitet. Sofern diese E-Mails dienstlich nicht angefordert wurden, werden sie ohne weitere Überprüfung gelöscht.

- Das Auftreten von sicherheitsrelevanten Ereignissen ist unverzüglich dem Fachbereich Inneres mitzuteilen. Dazu zählen unter anderem:
  - Verlust oder Veränderung von Dateien,
  - Verdacht auf Missbrauch von Benutzername und Passwort,
  - unerklärliches Systemverhalten und
  - Infizierung mit einem Computervirus.

6. Protokollierung der Nutzung

- Im Hinblick auf die Internetnutzung werden vom Fachbereich Inneres folgende Informationen gespeichert:
  - Rechnernummer (IP-Adresse),
  - Zieladresse und
  - aus dem Internet abgerufenes Datenvolumen.
- Die protokollierten Daten werden aus Sicherheitsgründen stichprobenartig überprüft. Bei begründetem Verdacht auf Missbrauch der Internet-Dienste durch eine Mitarbeiterin oder einen Mitarbeiter ist eine Verhaltenskontrolle unter Beteiligung des Personalrats zulässig.
- Der Fachbereich Inneres ist berechtigt und verpflichtet, PC stichprobenartig auf die Einhaltung dieser Dienstanweisung zu kontrollieren. Das gilt auch für PC mit einem vollen Internet-Zugang.

7. Verstöße

- Die Nichtbeachtung dieser Dienstanweisung gefährdet die über das PC-Netz der Organisation zugänglichen Daten auf zentralen und dezentralen Systemen.
- Ein grob fahrlässiger oder vorsätzlicher Verstoß gegen die Vorschriften dieser Dienstanweisung kann strafrechtlich verfolgt werden und darüber hinaus bei Arbeitern und Angestellten eine Verletzung ihres Arbeitsvertrages sowie bei Beamten ein Dienstvergehen darstellen.

8. In-Kraft-Treten

Diese Dienstanweisung tritt mit dem Tage der Unterzeichnung in Kraft.

Datum ……

Leiter der Organisation

Bestellformular backUP-Magazine für IT-Sicherheit	
***backUP*-Magazine erhalten Sie kostenlos!**	
Fax: 0431/988-1223 **Mail:** mail@datenschutzzentrum.de **Internet:** http://www.datenschutzzentrum.de	
Absender:	
Magazine:	
☐	**IT-Sicherheitskonzepte** Planung – Erstellung – Umsetzung
☐	**MS-Windows NT 4.0** Sicherheitsmaßnahmen und Restrisiken
☐	**MS-Windows NT 4.0** Resource Kit und Security Tools
☐	**MS-Windows 2000** Sicherheitsmaßnahmen und Restrisiken
☐	**PC-Arbeitsplatz** So viel Datenschutz muss an jedem Arbeitsplatz sein!
☐	**Bitte nehmen Sie mich in den Verteiler *backUP*-Magazine auf.**