Rheinische
Friedrich-Wilhelms-
Universität Bonn

Der Kanzler Dezernat 2
Datenverarbeitung und Kasse

Dienstanweisung

Datenschutz und Datensicherheit

beim Einsatz von IT-Systemen

in der Verwaltung der Universität Bonn

Stand: August 2006

Inhaltsverzeichnis:

§ 1:	Geltungsbereich, Zweck und Rechtsgrundlage	Seite	3
§ 2:	Verantwortlichkeit und Zuständigkeit	Seite	3
§ 3:	Allgemeines	Seite	4
§ 4:	Nutzung von Hardware und Software	Seite	5
§ 5:	Wartung/Fernwartung	Seite	6
§ 6:	Behandlung von Datenträgern	Seite	7
§ 7:	Zugriffsberechtigung	Seite	8
§ 8:	Zugangsberechtigung	Seite	9
§ 9:	Datensicherung	Seite	10
§ 10:	Datenübermittlung	Seite	10
§ 11:	Benutzungskennwörter (Passwörter)	Seite	11
§ 12:	Protokollierung	Seite	12
§ 13:	Interne Kontrolle	Seite	13
§ 14:	Inkrafttreten	Seite	13

§ 1
Geltungsbereich, Zweck und Rechtsgrundlage

I. Diese Dienstanweisung gilt für die Benutzung aller DV-Systeme und –Verfahren, die in der Verwaltung der Universität Bonn zum Einsatz kommen.

II. Diese Dienstanweisung dient dem Schutz und der Sicherung aller elektronisch gespeicherten personenbezogenen und betriebssensitiven Daten, die in der Universitätsverwaltung mittels elektronischer Datenverarbeitung verarbeitet werden.

III. Zum Schutz personenbezogener und betriebssensitiver Daten sind die bereichsspezifischen Gesetze (v.a. Teledienstedatenschutzgesetz (TDDSG) und Telekommunikationsgesetz (TKG)) sowie das geltende Datenschutzrecht zu beachten.

§ 2
Verantwortlichkeit und Zuständigkeit

I. Verantwortlich für die Behandlung der personenbezogenen Daten entsprechend der datenschutzrechtlichen Vorschriften ist die jeweils datenverarbeitende Stelle, also die Stelle, die veranlaßt hat, daß bestimmte Daten erhoben werden.

II. Die Institutionen, die aus dienstlichen Gründen elektronisch verarbeitete schutzwürdige Daten verarbeiten müssen, sind verantwortlich dafür, ob und inwieweit diese Daten an andere Einrichtungen der Universität Bonn oder Externe weitergegeben werden.
Die Weitergabe solcher Daten ist nur im Rahmen der gesetzlichen Bestimmungen und durch eine entsprechende schriftliche Anweisung der Fachabteilung an die DV-System- und Anwendungsbetreuer der Universitätsverwaltung möglich.

III. Jeder Beschäftigte der Universitätsverwaltung ist verpflichtet, sich über den Datenschutz zu informieren sowie die Bestimmungen dieser Dienstanweisung und die Regelungen der Datenschutzgesetze einzuhalten.

IV. Das Dezernat 2 (Datenverarbeitung) ist im Rahmen der Geschäftsverteilung u.a. zuständig für die DV-technischen Datenschutz- und Datensicherungsmaßnahmen der Universitätsverwaltung und hat alle technischen und organisatorischen Voraussetzungen zur Verhinderung von Beschädigung, Zerstörung, Verlust, Veruntreuung und Fehlleitung von Daten zu schaffen.

§ 3
Allgemeines

I. Der Einsatz neuer Verfahren sowie spätere Programmänderungen, soweit sie den fachlichen Inhalt des Verfahrens betreffen, bedürfen zusätzlich der formellen Einsatzerlaubnis, die durch den Kanzler bzw. durch das zuständige Fachdezernat erteilt wird. Hiervon ausgenommen sind reine Informationssysteme, die lediglich einer schnelleren Informationsbeschaffung dienen und keine Veränderung der Information zulassen (z.B. elektronische Nachschlagewerke).

II. Allen mit elektronischer Datenverarbeitung befaßten Beschäftigten ist es untersagt, schutzwürdige Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zu geben, zugänglich zu machen oder sonst zu nutzen. Dies gilt auch für die Zeit nach dem Beschäftigungsverhältnis an der Universität Bonn. Auf die Bestimmungen der §§ 33 (Straftaten) und 34 (Ordnungswidrigkeiten) des DSG NRW wird hingewiesen.

III. Um Mißbrauch bei der Verarbeitung von schutzwürdigen Daten zu verhindern, sind alle Beschäftigten der Universitätsverwaltung, die Zugang zu solchen Daten haben, zur Verschwiegenheit über diese Daten verpflichtet. Dies gilt auch für Informationen über Systemkommandos und deren Bestandteile, mit denen man sich Zugang zu schutzwürdigen Daten verschaffen kann. In besonderem Maße gilt dies für Passwörter.

§ 4
Nutzung von Hardware und Software

I. DV-Systeme der Universitätsverwaltung dürfen nur zu dienstlichen Zwecken genutzt werden.

II. Bei der Nutzung der Email über die DV-Systeme der Universitätsverwaltung sind die Regelungen der *Anlage 1* der *Geschäftsordnung für die Universitätsverwaltung* zu beachten. Diese Regelungen stehen im Intranet der Universität Bonn zur Einsichtnahme und zum Download bereit. Sie gelten sinngemäß auch für die Nutzung des Internets.

III. Räume mit DV-Ausstattung sind beim Verlassen grundsätzlich zu verschließen, um die Geräte so gegen unbefugten Zugriff oder Diebstahl zu schützen. Werden portable DV-Geräte wie Notebooks, Organizer und sonstige vergleichbare Geräte über einen längeren Zeitraum nicht genutzt, sind sie darüber hinaus inaktiv zu setzen bzw. einzuschließen.

IV. Die Einrichtung neuer Programme bzw. eine Veränderung der eingesetzten Programme darf nur durch die DV-System- und Anwendungsbetreuer der Universitätsverwaltung erfolgen bzw. bedarf deren Zustimmung.

V. Es dürfen nur freigegebene Programme eingerichtet werden. Die Freigabe erfolgt durch das Dezernat 2 (DV), nachdem eventuelle weitere Voraussetzungen, wie erfolgreicher Abschluß eines Mitbestimmungsverfahrens sowie die Zustimmung des Datenschutzbeauftragten vorliegen. Die Programmfreigabe und die Programmabnahme sind zu dokumentieren. Die Dokumentation ist an geeigneter Stelle zu hinterlegen, so daß sie jederzeit eingesehen werden kann.
Private Programme sowie Programme, die keinen Bezug zu dienstlichen Aufgaben haben, dürfen auf DV-Geräten der Verwaltung weder aufgespielt noch genutzt werden.

VI. Vor ihrem Einsatz ist sicherzustellen, daß die Programme frei von Computer-Viren und sonstiger Schadsoftware sind, in der geplanten Betriebsumgebung lauffähig und kompatibel zu den anderen eingesetzten Produkten sind, sowie

komplett einschließlich der erforderlichen Dokumentation ausgeliefert werden. Unterlagen und Datenträger sind geeignet zu sichern.

VII. Das Dezernat 2 (DV) führt ein Verzeichnis über die eingesetzten Anwendungsprogramme. Das Verzeichnis hat mindestens die Bezeichnung der Programme, die aktuelle Programmversion und das Datum der Erstinstallation zu enthalten.

VIII. Das Kopieren von Programmen ist mit Ausnahme der Erstellung von Sicherheitskopien untersagt, wenn urheberrechtliche Gründe dem entgegenstehen.

§ 5
Wartung/Fernwartung

I. Wartung sind alle Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Datenverarbeitungssysteme.

II. Bei Wartungsarbeiten darf grundsätzlich nicht auf personenbezogene Daten zugegriffen werden, es sei denn, dies ist für die Wartungsarbeiten unbedingt erforderlich.

III. Die erforderliche Wartung der Hard- und Software darf grundsätzlich nur durch die oder in Abstimmung mit den DV-Systembetreuern der Universitätsverwaltung oder dazu autorisierter Firmen erfolgen. Eigenständige Eingriffe in die Hardware oder Veränderungen der Hard- oder Software sind untersagt.
Bei Wartung durch externe Stellen ist eine schriftliche Vereinbarung erforderlich. Darin sind die im Rahmen der Wartung notwendigen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit einschließlich der Verpflichtung der mit den Wartungsarbeiten betrauten Personen zur Wahrung des Datengeheimnisses festzulegen.

IV. Eine Fernwartung ist in jedem Einzelfall frei zu schalten. Während der Fernwartung hat die zuständige Stelle besonders darauf zu achten, daß nur erlaubte Funktionen ausgeführt werden. Erforderlichenfalls ist die Fernwartung abzubre-

chen. Soweit möglich sind technische Ablaufprotokolle zu erstellen und für Kontrollzwecke zu sichern.

V. Änderungen der Betriebssysteme bzw. systemnaher Software während der Wartung sind erst nach Freigabe zu übernehmen. Die Änderungen sind zu dokumentieren.

§ 6
Behandlung von Datenträgern

I. Datenträger sind alle Medien, auf denen Daten gespeichert sind. Sie dürfen nur in Abstimmung mit dem Fachvorgesetzten aus dem Dienstbetrieb entfernt werden (z.B. für häusliche Arbeiten oder sonstige dienstliche Zwecke außer Haus). Bei personenbezogenen Daten gilt dies zusätzlich nur in begründeten Ausnahmefällen und mit Zustimmung des Personaldezernats. Im Übrigen hat der Nutzer eigenverantwortlich dafür zu sorgen, daß jeder Mißbrauch (z.B. Beschädigung, Weitergabe an Unbefugte) der entsprechenden Datenträger und Daten ausgeschlossen ist.

II. Vor dem Einlesen von Dateien von mobilen Datenträgern und dem Download von Dateien aus dem Internet sind diese auf Viren und sonstige Schadstoffsoftware (Trojaner, Würmer, Spyware etc.) hin zu untersuchen und ggfs. zu blockieren. Dies geschieht bei aktivierten Virenscannern in der Regel automatisch.

III. Beim Transport sind Datenträger zu verschlüsseln oder durch gleichwertige Maßnahmen zu schützen (verschlossene Behältnisse, Passwortschutz für Dateien, von Hand zu Hand etc.)

IV. Die Aufbewahrungsdauer zu archivierender Datenträger ist vom zuständigen Fachdezernat unter Berücksichtigung geltender Vorschriften schriftlich festzulegen.

V. Die Aufbewahrung von Datenträgern hat in gesicherten Behältnissen bzw. in gesicherten Räumen zu erfolgen, um unberechtigte Zugriffe zu verhindern.

VI. Kopien wichtiger System- und Anwendungsdateien sind an geeigneter Stelle auszulagern.

VII. Auf Datenträgern, die nicht mehr verwendbar sind oder verwendet werden oder deren Aufbewahrungsfrist nach Abs. IV abgelaufen ist, sind noch vorhandene Daten unwiederbringlich zu löschen. Die Vernichtung von Datenträgern darf nur durch die DV-System- und Anwendungsbetreuer oder durch zertifizierte Dienstleister in deren Auftrag erfolgen.

VIII. Sind bei Hardwarefehlern, insbesondere von Datenträgern (z. B. Festplatte), schutzwürdige Daten endgültig nicht reproduzierbar, so sind diese Daten durch die dem aktuellen technischen Stand entsprechenden Mittel unbrauchbar zu machen. Bei Gewährleistungsansprüchen gegenüber dem Hersteller bzw. dem Lieferanten ist dieser zur endgültigen Zerstörung der Daten zu verpflichten. Entsprechende Hinweise sind in die Verträge aufzunehmen.

§ 7
Zugriffsberechtigung

I. Der Zugriff auf Datenbestände der Universitätsverwaltung darf nur zur Erfüllung von Dienstaufgaben erfolgen.

II. Die Benutzer dürfen nur Zugriff zu den Daten und Programmen erhalten, die sie im Rahmen der ihnen übertragenen Aufgaben benötigen. Die Beantragung/Festlegung der Zugriffsberechtigungen – unterteilt nach Benutzer oder Nutzergruppen, benötigte Programme sowie die Art der Zugriffsberechtigungen (Lesen, Schreiben, Löschen, Ausführen) - erfolgt schriftlich durch den zuständigen Organisationsbereich an das Dezernat 2 (DV). Ähnliches gilt für das Löschen bzw. für das Ändern von Benutzer- und Emailkonten. Es ist wichtig, daß diese Informationen zeitnah und unaufgefordert an das Dezernat 2 (DV) weitergegeben werden. Entsprechende Formulare können im Intranet unter „Formulare – Dezernat 2“ abgerufen werden.

III. Die Einrichtung von berechtigten Benutzerkonten einschließlich der Übernahme der zugewiesenen Zugriffsrechte erfolgt durch die DV-System- bzw. durch die Anwendungsbetreuung des Dezernates 2 (DV).

IV. Bei der Verwendung von Passwörtern ist darauf zu achten, daß diese Unbefugten nicht bekannt werden. Hinsichtlich der weiteren Einzelheiten bzgl. des Umgangs mit Passwörtern vgl. § 11 dieser Dienstanweisung.

V. Jedem Benutzer im Verwaltungsnetz stehen zwei Netzlaufwerke für dienstliche Zwecke zur Verfügung. Das Laufwerk M: ist ein Benutzerlaufwerk, auf das nur der Benutzer selbst Zugriff hat, das Laufwerk N: dient als gemeinsamer Speicherbereich zum Datenaustausch innerhalb der jeweiligen Organisationseinheiten und im Vertretungsfall. Der dienstlich notwendige Zugriff auf das persönliche Laufwerk M: oder auf andere geschützte Dateien darf außer durch den Benutzer selbst nur mit dessen Einverständnis oder auf Antrag des jeweiligen Vorgesetzten durch die DV-Systembetreuung erfolgen. Der Vorgesetzte hat in seinem Antrag die Gründe für einen dienstlich notwendigen Zugriff schriftlich darzulegen. Der Mitarbeiter ist hierüber – wenn möglich – vorab zu informieren.

VI. Die Zugriffsberechtigung einschließlich der Vertretungsregelungen ist für jeden Anwendungsbereich schriftlich festzulegen.

§ 8
Zugangsberechtigung

I. Räume mit DV-Ausstattung sind beim Verlassen grundsätzlich zu verschließen. Räume mit mehr als einem Arbeitsplatz sind von der letzten Person, die den Raum verläßt, zu verschließen. DV-Endgeräte sind bei Dienstschluß nach vorschriftsmäßiger Programmbeendigung vollständig auszuschalten. Bei kurzfristiger Abwesenheit ist der Bildschirmarbeitsplatz softwaremäßig zu sperren.

II. Die Benutzer haben dafür Sorge zu tragen, daß bei Darstellung von personenbezogenen Daten auf Bildschirmen und Druckern Unbefugten die Einsicht verwehrt wird.

III. Die für die Systeme notwendigen zentralen Komponenten (Server, Hubs, Switches etc.) sind grundsätzlich in System-/Technikräumen unterzubringen. Zugangsberechtigt ist nur die DV-Systembetreuung des Dezernates 2 (DV).

§ 9
Datensicherung

I. Soweit die Daten zentral auf Servern gespeichert werden, erfolgt auch die Datensicherung zentral durch entsprechende Datensicherungssysteme arbeitstäglich. Die Sicherung der gespeicherten Daten ist zu protokollieren. Die Verantwortung hierfür obliegt den DV-Systembetreuern. Die Aufbewahrungsdauer der Sicherungen richtet sich nach der Art der Daten, gesetzlichen Vorgaben bzw. den Vorgaben der Anwender.

II. Den DV-System- und Anwendungsbetreuern ist der Zugriff auf jede Art von Daten nur zu Zwecken der Administration und der Benutzerbetreuung erlaubt.

III. Bei Einzelplatzsystemen bzw. in den Fällen, in denen Daten trotz Netzwerkverbindung lokal auf der jeweiligen DV-Anlage gespeichert werden, ist die Datensicherung durch den Benutzer selbst sicherzustellen. Sonst ist eine Wiederherstellung bei Problemen oder Defekten nicht mehr möglich.

§ 10
Datenübermittlung

I. Die Weitergabe von personenbezogenen Daten zu anderen Zwecken als denen, für die sie erhoben wurden, ist nur dann erlaubt, wenn eine Rechtsvorschrift oder die Wahrnehmung einer durch Gesetz oder Rechtsvorschrift zugewiesenen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt oder der Betroffene schriftlich eingewilligt hat. Die Datenweitergabe ist zu dokumentieren.

II. Der unverschlüsselte Versand personenbezogener Daten und Inhalte ist nur innerhalb des gesicherten Intranets der Universitätsverwaltung gestattet. Bis zur

Einführung entsprechender Verschlüsselungstechnik kann der externe E-Mail-Verkehr nicht als vertraulich gelten (siehe auch Geschäftsordnung für die Universitätsverwaltung – Anlage 1, Abschnitt 11).

§ 11
Benutzungskennwörter (Passwörter)

I. Um den Zugriff auf schutzwürdige Daten durch Unberechtigte zu verhindern, sind die Voraussetzungen dafür zu schaffen, daß die von den DV-Systemen gebotenen technischen Möglichkeiten des Kennwortschutzes genutzt werden.

II. Benutzungskennworte müssen mindestens 8-stellig sein. Sie dürfen nicht aus einer zu einfachen Ziffern- und/oder Buchstabenkombination, aus einfach abzuleitenden Begriffen oder leicht zu erratenden Namen (beispielsweise Namen von Angehörigen, Monatsnamen) bestehen. Es sollte eine Kombination aus Buchstaben, Ziffern und Sonderzeichen ohne erkennbare Gesetzmäßigkeit gewählt werden. Unterstützung bei der Vergabe von Benutzerkennwörtern leistet die DV-Systembetreuung der Universitätsverwaltung.

III. Die Benutzer haben darüber hinaus Folgendes zu beachten:

- Benutzungskennworte dürfen nur dann eingegeben werden, wenn die Eingabe nicht von Unbefugten beobachtet werden kann.
- Die Kennworte sind geheim zu halten. Es ist unzulässig, das Benutzungskennwort anderen Personen mitzuteilen oder zur Kenntnis gelangen zu lassen.
- Benutzungskennworte sollten nicht aufgeschrieben werden. Falls dies dennoch geschieht, ist dafür zu sorgen, daß keine andere Person die Möglichkeit erhält, diese Aufzeichnung einzusehen.
- Um die Vertraulichkeit der Benutzungskennworte zu gewährleisten, sind sie spätestens nach Ablauf der von der DV-Systembetreuung festzulegenden Gültigkeitsintervalle (systemabhängig) zu ändern. Die Gültigkeitsintervalle sollen drei Monate nicht überschreiten. Die Änderung des Benutzungskennwortes soll möglichst in unregelmäßigen Abständen erfolgen.

IV. Sind Benutzungskennworte Unbefugten bekannt geworden oder besteht ein entsprechender Verdacht, hat der Benutzer unverzüglich das Benutzungskennwort zu ändern oder eine Änderung zu veranlassen, falls er selbst nicht zur Änderung berechtigt ist. Beschäftigte, die Kenntnis von Benutzungskennworten erhalten haben, zu deren Benutzung sie nicht befugt sind, haben dies unverzüglich dem Benutzer und ihren Vorgesetzten mitzuteilen. Gegenüber weiteren Personen sind sie zur Geheimhaltung verpflichtet.

V. Alle Zugangsversuche zu DV-Systemen mittels falscher Benutzungskennworte werden vom Anmeldeserver protokolliert. Nach dreimaligem fehlerhaftem Zugangsversuch ist das Benutzerkonto zu sperren. Die Sperre kann nur durch die DV-Systembetreuung aufgehoben werden.

§ 12
Protokollierung

I. Die Protokollierung von Systemereignissen einschließlich der jeweiligen Benutzeridentifizierung dient der Datensicherheit und gehört zu den Maßnahmen der Speicher-, Benutzungs-, Zugriffs-, Sicherheits-, System- und Organisationskontrolle. Die so gewonnenen Protokolldaten werden nicht zur Anwesenheits- oder Leistungskontrolle herangezogen. Ihre Löschung erfolgt periodisch oder zyklisch durch automatische Überschreibung der jeweils ältesten Protokolldaten.

II. Nur in begründeten Verdachtsfällen auf Mißbrauch der DV-Systeme ist die DV-Systembetreuung in Zusammenarbeit mit der zuständigen Organisationseinheit und dem Personalrat befugt, die benutzerbezogenen Systemprotokolle in dieser Hinsicht auszuwerten, der Datenschutzbeauftragte ist ggfs. zu informieren.
Der Schutz der gespeicherten Systemprotokolle gegen unbefugten Zugriff ist gem. § 19 Abs. 2 Satz 2 DSG NW grundsätzlich durch technische Maßnahmen sicherzustellen.

III. Über besondere Erkenntnisse ist die Dienststellenleitung zu unterrichten.

§ 13
Interne Kontrolle

I. Die interne Kontrolle der Einhaltung dieser Dienstanweisung und sonstiger zum Datenschutz und zur Datensicherheit bestehender Vorschriften und Anweisungen wird von Dezernat 2 (DV) wahrgenommen, unbeschadet der Aufgaben und Befugnisse des Datenschutzbeauftragten. Berichte über Mängel/Feststellungen haben schriftlich zu erfolgen.

II. Die mit der internen Kontrolle beauftragten Beschäftigten haben im Rahmen ihrer Aufgaben nach dieser Dienstanweisung Zugangsberechtigung zu allen Räumen, in denen DV-Geräte aufgestellt sind.

§ 14
Inkrafttreten

I. Diese Dienstanweisung tritt mit sofortiger Wirkung in Kraft.

II. Sie ersetzt die Dienstanweisung „Datenschutz und Datensicherheit beim Einsatz von DV-Anlagen und –Geräten in der Verwaltung der Rheinischen-Friedrich-Wilhelms-Universität Bonn“ vom 21.10.1997.

Bonn, den 27. Juli 2006

Der Kanzler

.....

(Dr. R. Lutz)