UNIVERSITÄT SIEGEN

Dienstanweisung für Benutzer von DV-Geräten der Zentralen Universitätsverwaltung der Universität Siegen

Richtlinien und Vorgaben zu Datensicherheit und Datenschutz

Version 1.4 vom 01.10.2007

Inhaltsverzeichnis

1 Einleitung

1.1 Ziele

Ziel dieser Dienstanweisung ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Schutz- und Sicherheitsmaßnahmen Datenschutz und Datensicherheit auf das für die Zentrale Universitätsverwaltung erforderliche Niveau zu bringen.
Gefordert sind der Schutz und die Sicherheit der Daten, Programme und DV-Geräte der Zentralen Universitätsverwaltung. Besondere Aufmerksamkeit gilt den personenbezogenen Daten. Der Zugriff durch Unberechtigte ist zu verhindern. Dabei ist sowohl auf die Gefahren von außen als auch von innen zu achten.

1.2 Grundlagen

Diese Richtlinien und Vorgaben basieren auf folgenden Grundsatzdokumenten, welche im Dezernat 2 eingesehen werden können:

- IT-Grundschutzhandbuch des Bundesamt für Sicherheit in der Informationstechnik – Maßnahmen für den mittleren Schutzbedarf
- Bundesdatenschutzgesetz / Landesdatenschutzgesetz NW
- Allgemeine Dienstanweisung für den Umgang mit personenbezogenen Daten der Zentralen Universitätsverwaltung der Universität Siegen
- Dokumentation des Netzwerks der Zentralen Universitätsverwaltung der Universität Siegen
- Telekommunikationsgesetz

1.3 Über dieses Dokument

Dieses Dokument ist vor der Verabschiedung einer in Arbeit befindlichen, zentralen Datenschutzregelung für die gesamte Universität bzw. für die Zentrale Universitätsverwaltung erstellt. Sobald diese übergeordneten Regelungen in Kraft treten, wird dieses Dokument entsprechend angepasst.

Schreibweisen:
Zwecks größerer Übersichtlichkeit und besserer Lesbarkeit wird nur eine Form für die Bezeichnung für weibliche und männliche Personen verwendet. Angesprochen sind aber jeweils beide Gruppen.

2 Richtlinien für die Datensicherheit

2.1 Organisatorische Maßnahmen

- Die Arbeitsplatz-PCs dürfen für private Zwecke nur insoweit verwendet werden, als dienstliche Belange nicht entgegenstehen. Eine gesonderte Sicherung der Datenverarbeitung für private Zwecke zur Wahrung der Vertraulichkeit erfolgt nicht.
- Die Zuständigkeit für die Auswahl, die Installation und den Support von Hard- und Software liegt ausschließlich bei der Abteilung 2.4 - „IT-Anwendungen in der Zentralen Universitätsverwaltung". Eventuell dezentrale Entscheidungen sind in deren Vorfeld mit der Abteilung 2.4 abzusprechen.
- Das Ändern der Hard- und Softwarekonfiguration erfolgt ausschließlich durch die Abteilung 2.4. Eingriffe jeglicher Art sind nicht gestattet. Unautorisierte Veränderungen an den eingesetzten Programmen sind untersagt.
  Die Inventarisierungsaufkleber dürfen nicht entfernt oder ausgetauscht werden.
- Das Einbringen privater Hard- und / oder Software ist nicht zulässig. Insbesondere sind die Installation und Verwendung eigener Software auf hochschuleigenen Computern und das Anschließen privater Persönlicher Digitaler Assistenten (PDA/MDA) verboten. Die Mitarbeiter der Abteilung 2.4 sind angehalten, mittels Sichtprüfung regelmäßig Kontrollen durchzuführen.
- Für die Anbindung des Organizer-Teils von Mobiltelefonen mit entsprechender Funktionalität gelten die folgenden speziellen Vorgaben:
  - Verwendet werden dürfen ausschließlich von der Abteilung 2.4 freigegebene und vom Dezernat 5 zentral beschaffte Mobiltelefone. Die Verantwortung für die Hardware, z. B. bzgl. Reparatur oder Ersatz, liegt ebenfalls im Dezernat 5.
    Wichtig ist die Konzentration auf eine Produktlinie eines Herstellers. Auf häufige Modell- und Softwareversions-Wechsel ist zu verzichten. Die Abstimmung mit der Abteilung 2.4 wird vorausgesetzt.
  - Auf Grund der technischen Vorgaben für die Verwaltungs-IT insgesamt ist eine Anbindung nur über kabelgebundene serielle Anschlüsse, nicht aber über andere Kommunikationswege, wie beispielsweise USB, gestattet.
  - Als Betriebssystem ist nur *MS Windows Mobile* erlaubt.
  - Für die Anbindung der Mobiltelefone an die PCs der Verwaltungs-IT und die Sicherung dieser Anbindung zum Schutz des Netzwerks der Verwaltung ist ausschließlich die Abteilung 2.4 zuständig.
  - Verwendet werden darf nur die Anwendung *MS ActiveSync* zum Datenabgleich zwischen MS Outlook auf dem PC und MS Outlook auf den Mobiltelefonen. Eine Übertragung anderer Daten ist verboten. Die Synchronisation erfolgt gemäß definierter Profile.
  - Ist die Mobiltelefon-Hard- und / oder -Software zur eingesetzten Arbeitsplatz-Software nicht kompatibel bzw. sind Störungen nicht ausgeschlossen, kann die Anbindung abgelehnt werden.
  - Mit den Geräten ist sorgsam und sachgerecht umzugehen. Für die Synchronisation, die Datensicherung und -wiederherstellung und den Datenschutz ist der Benutzer selbst verantwortlich.
  - Die für den Dienstgebrauch bereit gestellten Mobiltelefone mit Organizer-Teil dürfen nicht mit privaten PCs synchronisiert werden.
- Die Entwicklung von Anwendungen ist ausschließlich für den betrieblichen Bedarf und nur mittels zugelassener Standardsoftware erlaubt. Dazu ist eine Abstimmung mit der Abteilung 2.4 erforderlich.
- Die eingesetzten Programme sind rechtlich geschützt. Unberechtigte Benutzung, Vervielfältigung oder Verteilung bedeuten eine Verletzung dieser Schutzrechte und sind nicht gestattet.

- Der Zugang zum Internet dient dienstlichen Aufgaben. Es ist diesbezüglich mit Kontrollen vor Ort an den Arbeitsplatz-PCs zu rechnen. Laden Sie nur Dateien aus vertrauenswürdigen Quellen herunter und unterziehen Sie sie umgehend einer Virenprüfung. Der Nutzer haftet für den durch die unerlaubte Nutzung entstandenen Schaden.
  Die Installation von Zusatz- bzw. Hilfsprogrammen (AddOns und PlugIns) ist nicht erlaubt.
- Nach Dienstende bzw. bei längerem Verlassen des Arbeitsplatzes ist der Arbeitsplatz-PC auszuschalten. Stellen Sie auf jeden Fall sicher, dass über Nacht PC und Monitor nicht angeschaltet sind.

2.2 Schutz und Wiederherstellbarkeit der Arbeitsplatz-PCs

- Das Ablegen von Arbeits-Daten hat ausschließlich auf den Servern zu erfolgen. Auf der Festplatte der Arbeitsplatz-PCs sind keinerlei Arbeits-Daten zu speichern, da diese nicht gesichert werden. Wenn alle Daten auf den Servern des Verwaltungsrechenzentrums abgelegt werden, droht im Falle eines nichtbehebbaren Hard- oder Softwareproblems kein Datenverlust.
- Standardmäßig werden auch die nutzerspezifischen Informationen auf dem Server abgelegt, um diese nach einem Systemschaden an einem Arbeitsplatz-PC wieder zur Verfügung zu haben. Diesbezügliche Voreinstellungen sollten also nicht verändert werden.
- Die umfangreiche Neuinstallation der kompletten Arbeitsplatz-PC-Software würde mehrere Stunden Arbeitsausfall und evtl. den Verlust nutzerspezifischer Informationen / Einstellungen bedeuten. Eine schnelle Wiederherstellung eines definierten Standes von Betriebssystem und Anwendungsprogrammen bei Zerstörung der Softwareinstallation wird daher durch die Verwendung von Festplattenimage-Dateien gewährleistet.
- Mit Hilfe von Virenschutzprogrammen sollte periodisch eine Überprüfung auf Virenbefall vorgenommen werden. Dazu sind alle Bereiche der Festplatten mit dem lokal installierten Virenscanner zu kontrollieren. Besondere Aufmerksamkeit gilt dabei Dateien, die aus anderen Einrichtungen kommen. Die Mitarbeiter, denen die Nutzung ihres Diskettenlaufwerks / eines CD-Laufwerks erlaubt ist, müssen vor dem ersten Zugriff auf eine Diskette / CD **immer** eine Virenprüfung durchführen.
  Schalten Sie die eingerichtete Automatisierung dieser Funktionen nie ab!
  Es sind ständig die aktuellen Virensignatur-Files zu verwenden. Diese werden von der Arbeitsplatz-PC-Software - ebenfalls automatisch - aus dem Internet bezogen.

Sollte ein Virus auf einen Arbeitsplatz-PC gelangt sein, ist **sofort** die Hotline der Abteilung 2.4 - Tel.: 4999 - zu informieren, auch wenn der Virus durch das Virenschutzprogramm entfernt wurde.

2.3 Allgemeine Verhaltensregeln

- Speisen und Getränke sollten nicht in der Nähe von DV-Geräten zu sich genommen werden. Besondere Vorsicht gilt beim Umgang mit Flüssigkeiten insgesamt.
- Beim Betrieb anderer elektronischer Geräte sollte auf einen entsprechend großen Abstand geachtet werden, um störende elektrische Einflüsse zu vermeiden.

3 Richtlinien für den Datenschutz

3.1 Organisatorische Maßnahmen

- Die regelmäßige Übermittlung von Daten aus dem Netzwerk der Zentralen Universitätsverwaltung heraus - gleich in welcher elektronischen Form - bedarf einer einmaligen, prinzipiellen Genehmigung durch den Datenschutzbeauftragten bzw. durch den Kanzler.
  Es ist besonders darauf zu achten, an wen Mails gesendet werden - speziell bei der Verwendung von Verteilerlisten - und welche Dateien als Anlage beigefügt sind.
- Das „Mithören" oder Stören von Datenübertragungen ist, außer zum Zweck der Fehlerverfolgung durch das Hochschulrechenzentrum nach Bekanntgabe, nicht gestattet.
- Die Nutzung hochschuleigener Hard- und / oder Software außerhalb der Hochschule ist nur mit vorher schriftlich erteilter Zustimmung des jeweiligen Dezernenten und der Information der Abteilung 2.4 gestattet. Es gelten die Regeln zur Datensicherheit in besonderer Schärfe. Der Zugang zu außerhalb der Dienstgebäude eingesetzten Geräten ist für Unbefugte auszuschließen. Dazu zählen auch Familienangehörige! Alle entnehmbaren Datenträger sind verschlossen aufzubewahren.
- Jeder Mitarbeiter darf nur auf Programme und Daten zugreifen, die er zur Erfüllung seiner Arbeitsaufgaben benötigt.
- Dem Benutzerservice und den Systemadministratoren ist es erlaubt, im Rahmen ihrer Aufgabenstellung und nach vorheriger Zustimmung durch den Anwender über Fernbedienungsprogramme auf dessen Computer zuzugreifen.
- Den Benutzern ist der Zugriff auf Disketten wegen der Beschreibbarkeit des Mediums verwehrt. Müssen Daten von Disketten gelesen werden, hat dies über einen PC der Systemadministration zu erfolgen.
  Welche Mitarbeiter zur Erledigung ihrer Arbeitsaufgaben von dieser Regelung auszunehmen sind, entscheiden die Abteilungsleiter. Eine Begründung ist erforderlich.
- Wird für die tägliche Arbeit kein CD-Laufwerk benötigt und ist deshalb nicht installiert, können Daten von CD an den PCs der Mitarbeiter der Abteilung 2.4 eingelesen werden lassen, wenn dies erforderlich ist.
- Regelungen bzgl. Email-Posteingang bei Abwesenheit
  In Ergänzung § 17 der Geschäftsordnung für die Zentrale Universitätsverwaltung der Universität Siegen vom 22. Mai 2006

  „Die E-Mails sind möglichst einmal täglich abzufragen und zügig zu beantworten oder ggf. weiterzuleiten. Bei Abwesenheit sind geeignete Maßnahmen zu treffen (Abwesenheitsassistent, Einräumen von Leserechten auf das eigene Postfach). E-Mails von grundsätzlicher Bedeutung sind der/dem Vorgesetzten durch Weiterleiten der E-Mail oder Aufnahme in den Antwort-Verteiler zur Kenntnis zu geben."

  gelten bei einer Abwesenheit von mehr als 3 Tagen folgende Regelungen:

  1) <u>Geplante Abwesenheit</u>

  Im Falle einer geplanten Abwesenheit (Urlaub, geplanter Krankenhausaufenthalt, Kur etc.) ist mit der Vertretung auch das genaue Vorgehen bzgl. Email-Posteingang für den Zeitraum der Abwesenheit zu vereinbaren.

  Die Vertretung muss alle für den Abwesenden eingehenden Emails einsehen können. Dies zu gewährleisten gibt es zwei Möglichkeiten. Empfohlen wird Variante a).

  a) Die Vertretung erhält direkten Zugriff auf den Email-Posteingang des Abwesenden und antwortet ggf. in dessen Namen.
  i. Freigeben des Posteingangs durch den Vertretenen **vor Beginn** der Abwesenheit
  ii. Verbinden des freigegebenen Posteingangs durch die Vertretung
  iii. Entfernen der Freigabe des Posteingangs durch den Vertretenen nach Ende der Abwesenheit

b) Weiterleitung einer Kopie aller eingehenden Emails per Outlook-Regel an den Vertreter
   i. Aktivieren einer entsprechenden Regel im Outlook-Abwesenheitsassistenten durch den Vertretenen **vor Beginn** der Abwesenheit
   ii. Deaktivieren der Regel im Outlook-Abwesenheitsassistenten durch den Vertretenen nach Ende der Abwesenheit

Bitte beachten Sie, dass die Emails im Posteingang des Vertretenen als "ungelesen" markiert bleiben, auch wenn der Vertreter seine Kopie der Email gelesen hat. Eine genaue Absprache der Vorgehensweise ist unbedingt erforderlich!

Hat die/der Abwesende vergessen, eine der beiden Varianten einzurichten, hat die Vertretung die/den zuständige/n Dezernentin/Dezernenten zu informieren. Die Anforderung bei Abteilung 2.4 muss schriftlich und mit Unterschrift der Dezernentin/ des Dezernenten bzw. per persönlicher Email der Dezernentin/des Dezernenten an den Abteilungsleiter 2.4 erfolgen. Die/der Abwesende sollte vorab telefonisch informiert werden.

Außerdem sollte vom Abwesenden im Outlook-Abwesenheitsassistent immer die automatische Benachrichtigung über die Abwesenheit aktiviert werden. Diese sollte unbedingt auch den Namen, die Telefonnummer und die Email-Adresse der Vertretung enthalten.

Beispiel:

Sehr geehrte Damen und Herren,

ich bin zurzeit nicht im Hause. Ich werde Ihre E-Mail nach meiner Rückkehr beantworten. Bitte wenden Sie sich bis dahin an meine Vertretung, Herrn Müller, Tel.: 0271/740-xxxx, mailto:max.mueller@zv.uni-siegen.de.

Mit freundlichen Grüßen

2) Unvorhersehbare Abwesenheit

Der Outlook-Abwesenheitsassistent kann nur vom Postfach-Inhaber selbst aktiviert werden. Um aber im Falle einer unvorhersehbaren Abwesenheit (Krankheit) dennoch die Vertretung auch bzgl. Bearbeitung der eingehenden Emails zu gewährleisten, hat die Vertretung die nachträgliche Einrichtung von Variante 1a) durch die Abteilung 2.4 mit der zuständigen Dezernentin/dem zuständigen Dezernenten abzustimmen. Die Anforderung hat schriftlich und mit Unterschrift der Dezernentin/des Dezernenten bzw. per persönlicher Email der Dezernentin/des Dezernenten an den Abteilungsleiter 2.4 zu erfolgen. Die/der Abwesende sollte vorab telefonisch informiert werden.

Melden Sie Störungen bitte umgehend der Abteilung 2.4 unter der Hotline Tel.: 4999.

3.2 Administrative Festlegungen

- Die Möglichkeit zur lokalen Anmeldung ist nur dem lokalen Administrator und dem Inhaber des Arbeitsplatzes gegeben.
- Die minimale Passwortlänge beträgt 8 Zeichen, die maximale 14. Zwischen Groß- und Kleinschreibung wird unterschieden. Verwendet werden sollten neben Zahlen und Buchstaben auch Sonderzeichen.
- 3 Fehlversuche bei der Passworteingabe führen zu 30 min Anmelde-Sperre oder vollständiger Sperrung des Benutzerkontos.
- Die Anmeldezeit für die Nutzer ist Mo. - Fr. auf die Zeit von 6.30 - 22.00 Uhr festgelegt. Am Samstag und Sonntag ist die Anmeldung nur in der Zeit von 8:00 bis 16:00 Uhr erlaubt.

3.3 Richtlinien und Vorgaben für Benutzer

- Ihr Passwort dient neben dem Schutz des Systems auch Ihrer eigenen Absicherung. Verschafft sich ein Unberechtigter mit Hilfe Ihrer Benutzerkennung Zugang, sind Sie in der Verantwortung.
  Geben Sie ihr Passwort an niemanden weiter. Merken Sie sich Ihre Passwörter gut, notieren Sie sie aber nicht.
- Ändern Sie Ihre Passwörter auch ohne Aufforderung, wenn Sie glauben, dass sie anderen Personen bekannt geworden sein könnten.
- Verwenden Sie als Passwort eine Kombination aus min. 8 Buchstaben, Sonderzeichen und Zahlen, die keinen Sinn ergibt. Namen, Gegenstände aus Ihrem Umfeld bzw. Wörter, die in irgendeinem Wörterbuch stehen, sollten nicht als Passwort dienen.
- Verlassen Sie Ihren Arbeitsplatz, ist der Arbeitsplatz-PC zu sperren. Betätigen Sie dazu die Tasten Strg + Alt + Entf und Bestätigen Sie anschließend mit der Enter-Taste. Damit ist Ihre Anzeige auch vor unerwünschten Blicken Unberechtigter geschützt.
- Arbeits-Daten sind ausschließlich auf dem Server abzulegen. Lokal gespeicherte Daten bilden immer ein Risiko. Bedenken Sie auch, dass die Betriebssysteme über eine lokale Papierkorb-Funktion verfügen, die ein leichtes Wiederherstellen vermeintlich gelöschter Dokumente ermöglicht.
- Legen Sie regelmäßig Sicherungen Ihrer aktuellen Arbeit an. Nutzen Sie die "Automatisch speichern..." - Funktion vieler Anwendungen, um den Schaden bei plötzlichem Stromausfall zu begrenzen.
- Verändern Sie niemals irgendwelche System-Dateien. Sollten Änderungen an den Einstellungen notwendig sein, informieren Sie die Abteilung 2.4.

Erscheint Ihnen irgendetwas ungewohnt oder gar verdächtig, ist ebenfalls umgehend die Abteilung 2.4 zu informieren. Achten Sie ggf. beim Anmelden darauf, ob der Ihnen angezeigte letzte Anmeldename stimmt. Achten Sie auf Ihre Dateien. Findet sich darunter etwas, was Sie sicher nicht dorthin getan haben, so wenden Sie sich an die Administratoren.

4 Verbindlichkeiten und Kontrolle

Diese Richtlinien und Vorgaben sind für alle Mitarbeiter der Zentralen Universitätsverwaltung verbindlich, die im Rahmen Ihrer Tätigkeit DV-Geräte einsetzen. Die Dienststelle kommt ihrer Informationspflicht den Bediensteten gegenüber nach.
Als Zeichen der Kenntnis dieser Richtlinien und Vorgaben und ihrer Akzeptierung ist von allen betroffenen Mitarbeitern eine entsprechende Verpflichtungserklärung zu unterzeichnen, welche allen Mitarbeitern in Papierform zuzuleiten ist. Nach Eingangskontrolle durch das Dezernat 2 wird sie dem Dezernat 4 zur Ablage in der Personalakte zugeleitet.
Über spätere Änderungen, Ergänzungen und Neufassungen, die an zentraler Stelle veröffentlicht werden, benachrichtigt die Abteilung 2.4 die Mitarbeiter, welche sich dann selbst informieren.

Die noch zu benennenden Verantwortlichen sind verpflichtet, die Einhaltung dieser Richtlinien und Vorgaben zu kontrollieren.

Verstöße gegen die Bestimmungen dieser Dienstanweisung können straf-, zivil- und arbeits- bzw. dienstrechtliche Konsequenzen haben. Auf die §§ 33, 34 des Datenschutzgesetzes NW, welche als Anhang beigefügt sind, wird besonders hingewiesen.
Mit einer Kontrolle der Einhaltung erfolgt keine Leistungskontrolle.

Mindestens jährlich führt die Abteilung Datenverarbeitung Informationsveranstaltungen durch, auf denen Details erläutert und Fragen beantwortet werden. Alle von der Dienstanweisung Betroffenen nehmen an einer dieser Veranstaltungen teil.

Ausnahmegenehmigungen, die teilweise von der Einhaltung dieser Richtlinien befreien, können nur vom (noch zu schaffendem) zentralen Datenschutz-Gremium der Zentralen Universitätsverwaltung erteilt werden und bedürfen der Schriftform.

Siegen, den 26.09.2007

J. P. Sch.

(Dr. Johann Peter Schäfer)

5 Anhang

Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen – DSG NW –)

Vierter Teil
Straf- und Bußgeldvorschriften

§ 33

Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, entgegen den Vorschriften über den Datenschutz in diesem Gesetz oder in anderen Rechtsvorschriften des Landes Nordrhein-Westfalen personenbezogene Daten, die nicht offenkundig sind,

a. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,
b. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht. Der Versuch ist strafbar.
(2) Absatz 1 findet nur Anwendung, soweit die Tat nicht nach anderen Vorschriften mit Strafe bedroht ist.

§ 34

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften über den Datenschutz in diesem Gesetz oder in anderen Rechtsvorschriften des Landes Nordrhein-Westfalen personenbezogene Daten, die nicht offenkundig sind,

a. erhebt, speichert, zweckwidrig verwendet, verändert, weitergibt, zum Abruf bereithält oder löscht,
b. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst.

Ordnungswidrig handelt auch, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 100.000 Deutschen Mark oder 50.000 Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist für die Verfolgung und Ahndung von Ordnungswidrigkeiten

a. nach den Absätzen 1 und 2 die Bezirksregierung,
b. nach § 44 des Bundesdatenschutzgesetzes der Landesbeauftragte für den Datenschutz.