Die IT-Sicherheitsrichtlinien der Universität Göttingen

- Einführung für Anwender -

von

Dr. Holger Beck

IT-Sicherheitsbeauftragter der GWDG
Leiter der Arbeitsgruppe IT-Sicherheit der Universität Göttingen
http://it-sicherheit.uni-goettingen.de

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Am Fassberg, 37077 Göttingen

Fon: 0551 201-1510 Fax: 0551 201-2150
gwdg@gwdg.de www.gwdg.de

IT-Sicherheit

- Sicherheit der Informationstechnologie, also von
  - **Informationen,**
    - d.h. Dateien, Datenbanken und deren Inhalten,
  - **Geräten** zur Verarbeitung der Informationen,
    - insbesondere Computer, und
  - **Infrastrukturen**
    - z.B. Netzwerk,
- zur Gewährleistung von
  - **Vertraulichkeit**,
  - **Verfügbarkeit**,
  - **Integrität**

GWDG

IT-Sicherheitsrichtlinien der Universität

- **Organisationsrichtlinie zur IT-Sicherheit**

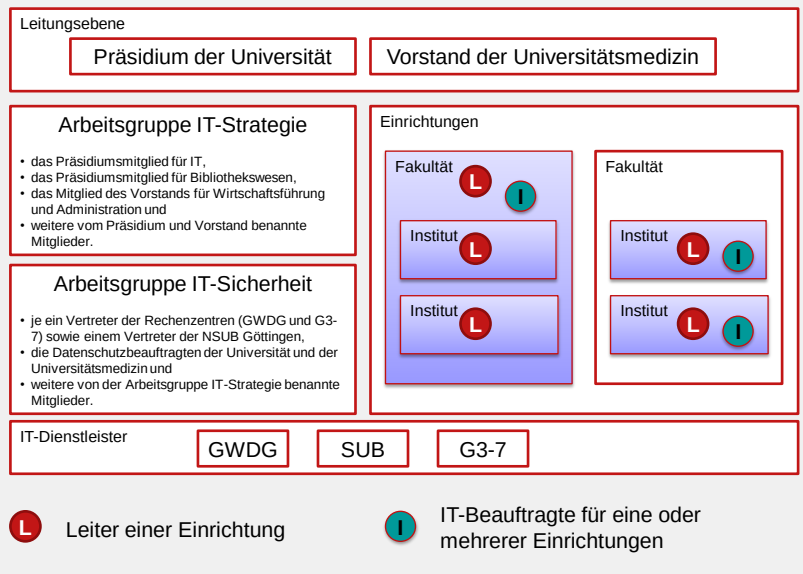
  1. Gegenstand der Richtlinie
  2. Geltungsbereich
  3. IT-Sicherheitskonzept
  4. Organisationsstruktur des IT-Sicherheitsprozesses
  5. Aufgaben der Beteiligten
  6. Gefahrenintervention
  7. Finanzierung
  8. Inkrafttreten

- **Sicherheitsrahmenrichtlinie**

  1. Vorbemerkungen
     - Grundschutz bei niedrigem bis mittlerem Schutzbedarf
     - Hinweis auf Möglichkeit und Bedingung für Ausnahmen
  2. Maßnahmen des IT-Grundschutzes für IT-Anwender
     - 20 Maßnahmen auf 6 Seiten
     - Faltblatt
  3. Maßnahmen des IT-Grundschutzes für IT-Personal
     - 51 Maßnahmen auf 16 Seiten

GWDG

Organigramm



Zum Maßnahmenkatalog

- **Beschränkung auf das Notwendige**
  - Aufgreifen allgemein anerkannter Standards.
  - Viele Maßnahmen sind so weit schon Stand der Technik, dass sie schon umgesetzt sein dürften.
  - Trotzdem verbleiben unangenehme oder ungeliebte Maßnahmen.
- **Arbeitserleichterungen** durch Standardisierung
  - Nutzen Sie die Richtlinien als Checkliste
- IT-Sicherheit ist ein **Prozess**
  - Die Richtlinien sind nicht in Ewigkeit unveränderlich
  - Beteiligung aller IT-Nutzer
- Unterteilung
  - Maßnahmen für **Anwender**, die nur IT nutzen
  - Maßnahmen für **IT-Personal**, d.h. alle Personen, die Rechner oder Anwendungen konfigurieren, installieren, …

5

Maßnahmen zum IT-Grundschutz für IT-Anwender

A.1 Anwenderqualifizierung
A.2 Meldung von Sicherheitsproblemen
A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen
A.4 Räumlicher Zugangsschutz
A.5 Sicherung mobiler Computer
A.6 Kontrollierter Softwareeinsatz
A.7 Keine private Hard- und Software
A.8 Virenschutz
A.9 Abmelden und ausschalten
A.10 Personenbezogene Kennungen
A.11 Gebrauch von Passwörtern
A.12 Zugriffsrechte
A.13 Netzzugänge
A.14 Telearbeit
A.15 Sichere Netzwerknutzung
A.16 Datensicherung
A.17 Umgang mit Datenträgern
A.18 Physisches Löschen von Datenträgern
A.19 Schützenswerte Daten auf dem Arbeitsplatzrechner
A.20 Sichere Entsorgung vertraulicher Papiere

6

IT-Sicherheit– Wieso?

- **Computer und IT vereinfachen das Leben**
  - **Schneller Zugriff** auf Informationen
  - **Schnelle Produktion** von Dokumenten
  - **Schnelle Kommunikation** über Netze
- **Was ist das Internet?**
  - **WWW** – eine **riesige Informationsquelle**?
  - **E-Mail** – schneller als Brief und Fax?
  - **E-Business** – einfacher, billiger, bequemer Geschäfte machen?
  - **Unterhaltungsmedium** – flexibler und vielfältiger als Fernsehen und Radio?
  - **Downloads** – eine unerschöpfliche Quelle frei verfügbarer Programme?
- **ja** – **aber**!

7

Unsicherheit der IT – darum!

- **Noch nie erlebt – noch nie gehört?**
- **Rechnerprobleme**
  - **defekte Rechner**
  - **gelöschte Dateien**
  - **gestohlene Rechner**
- **Netzwerkprobleme**
  - **Viren**, die Rechner und Netze lahm legen?
  - **Geklaute Zugangsdaten** zum Konto?
  - **Einbrüche** in Rechenanlagen?
  - **Software die – böswillig** – etwas ganz anderes tut als versprochen?
  - **Überfüllte Briefkästen**?

8

Angst vor Computern und Internet?

- **Angst** – **nein**!
- **Vorsicht** – **ja**!
- **Sicherer Umgang mit Computern und Internet**
  - Gefahren kennen,
  - sich auf Gefahren einstellen,
  - Sicherheitsregeln und verfügbare Schutzmaßnahmen anwenden
- **Ziel des Kurses**
  - **Sensibilisierung** für die Gefährdungen,
  - **Grundregeln** vermitteln.
  - Sie sollen nicht alles selbst können, aber wissen, wo Sie Hilfe benötigen.
- Vertiefung (Bits und Bytes) in weiteren Kursen

Das lässt sich ja alles wieder reparieren! (?)

- **Schäden**
  - Rechner und Netze zeitweise **nicht mehr funktionsfähig**,
  - Wiederherstellung **kostet viel Zeit**,
  - aber meist keine weitergehenden Schäden.
  - **Abbuchungen von Ihrem Konto** über Telefonrechnungen oder direkt durch ausspionierte Zugangsdaten sind noch selten
- **Aber** schon
  - **die nächste Virenattacke**
    - könnte nicht nur Netze und Mailserver überlasten,
    - sondern zu **Totalverlusten von Daten** führen,
  - **das nächste Trojanische Pferd**
    - könnte **Zugriff auf sensible Daten** erlauben,
  - **der nächste Einbrecher**
    - könnte Ihren Rechner nicht nur als **illegale Tauschbörse** für Filme und Software,
    - sondern auch als Server für **Kinderpornographie** missbrauchen
    - und Sie müssen beweisen, dass Sie den nicht selbst eingerichtet haben.
  - **die nächste Phishing-Attacke**
    - kann Ihr **Konto plündern**

A.1 Anwenderqualifizierung

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Beauftragter

Die Mitarbeiter sind **aufgabenspezifisch zu schulen** und dürfen erst dann mit IT-Verfahren arbeiten.

Dabei sind sie insbesondere auch mit den für sie geltenden **Sicherheitsmaßnahmen und den Erfordernissen des Datenschutzes** vertraut zu machen.

Die Schulung hat prinzipiell auch das allgemeine **Sicherheitsbewusstsein** und die Einsicht in die Notwendigkeit von IT-Sicherheitsmaßnahmen zu entwickeln.

Die Schulung sollte auch eine **realistische Selbsteinschätzung** fördern. Die Anwender sollten erkennen, wann Experten hinzugezogen werden sollten.

11

A.2 Meldung von Sicherheitsproblemen

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Beauftragter

Auftretende **Sicherheitsprobleme aller Art** (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u.a.) **sind dem zuständigen IT-Personal mitzuteilen**. Jeder schwerwiegende Vorfall ist zu dokumentieren und der Arbeitsgruppe „IT-Sicherheit“ zu melden.

12

A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen

Verantwortlich für Initiierung: Bereichsleitung
Verantwortlich für Umsetzung: Bereichsleitung

Verstöße werden nach den geltenden rechtlichen Bestimmungen geahndet.

Als Verstoß gilt die **vorsätzliche oder grob fahrlässige Nichtbeachtung** der IT-Sicherheitsrahmenrichtlinie, insbesondere wenn sie

- die Sicherheit der Mitarbeiter, Nutzer, Vertragspartner, Berater und des Vermögens der Universität Göttingen in erheblichen Umfang beeinträchtigt,
- der Universität Göttingen erheblichen finanziellen Verlust durch Kompromittierung der Sicherheit von Daten oder Geschäftsinformationen einbringt,
- den unberechtigten Zugriff auf Systeme und Informationen, deren Preisgabe und/oder Änderung beinhaltet,
- die Nutzung von Informationen der Universität Göttingen für illegale Zwecke beinhaltet und
- den unbefugten Zugriff auf personenbezogene Daten ermöglicht.

Beurteilung und Ahndung eines Verstoßes erfolgen für Mitarbeiter der Universität in jedem Einzelfall unter **Beteiligung des Personalrates**.

Zur **Gefahrenintervention** können entsprechend der Organisationsrichtlinie zur IT-Sicherheit von den IT-Beauftragten oder den Rechenzentren Netzzugänge oder Benutzerkonten vorübergehend stillgelegt werden.

A.4 Räumlicher Zugangsschutz

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Der **unbefugte Zugang zu Geräten** und die unbefugte Nutzung der Informationstechnik muss verhindert werden.

Bei Abwesenheit sind **Mitarbeiterräume** mit Informationstechnologie **verschlossen zu halten**.

Bei der Anordnung und baulichen Einrichtung der Geräte ist darauf zu achten, dass schützenswerte **Daten nicht von Unbefugten eingesehen** werden können.

Beim **Ausdrucken** derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

A.5 Sicherung mobiler Computer

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Anwender

Bei der Speicherung von **schützenswerten Daten** auf mobilen Computern (Notebooks) sind besondere Vorkehrungen zum Schutz der Daten zu treffen. Die Dateien **müssen verschlüsselt werden**.

Notebooks sind möglichst **verschlossen aufzubewahren**.

Auf **Datensicherung** ist besonders Wert zu legen.

15

A.6 Kontrollierter Softwareeinsatz

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Anwender

Auf Rechnersystemen der Universität Göttingen darf zum Zweck des Schutzes von universitätseigener Hardware und dem Universitätsnetz nur Software installiert werden, die zur **Erfüllung der dienstlichen Aufgaben** erforderlich ist.

Das **eigenmächtige Einspielen**, insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software, ist nur gestattet, wenn sichergestellt ist, dass von dieser Software **keine Gefährdung für das IT-System bzw. das Datennetz** ausgeht.

Im Zweifelsfall ist die **Zustimmung der Leitung** der betreffenden Organisationseinheit einzuholen.

16

A.7 Keine private Hard- und Software

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Anwender

Die Benutzung von **privater Hard- und Software** in Verbindung mit technischen Einrichtungen der Universität Göttingen und deren Netzen **ist grundsätzlich nicht gestattet**.

Die **Leitung der betreffenden Organisationseinheit kann Ausnahmen gestatten**.

Allgemeine Ausnahmen gelten für den Einsatz von privaten Computern für **Lehrveranstaltungen** und Vorträge sowie in speziell **gekennzeichneten Bereichen**, wie zum Beispiel in Bibliotheken oder in Studierendenarbeitsbereichen, und im Funknetz GoeMobile.

17

A.8 Virenschutz

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Auf allen Arbeitsplatzrechnern ist, soweit technisch möglich, ein **aktueller Virenscanner** einzurichten, der automatisch alle eingehenden und zu öffnenden Dateien überprüft. Damit soll bereits das Eindringen von schädlichen Programmen erkannt und verhindert werden.

Per E-Mail erhaltene **Anhänge** sind nur dann zu öffnen, wenn ihre Herkunft und Ungefährlichkeit sichergestellt ist.

Bei Verdacht auf Vireninfektion ist das zuständige IT-Personal zu informieren.

18

Auch Sie sind gefährdet!

- **Viren und Würmer**
  - Virenverbreitung durch E-Mail
  - Wurmangriffe direkt über Netz
  - Gefährdung der Stabilität und Integrität der Rechner und Netze.
- **Trojanische Pferde**
  - von Viren und Würmern hinterlassen,
  - von Internetseiten unbeabsichtigt heruntergeladen,
  - Ausspähen vertraulicher Informationen (Kennwörter, Kreditkarteninformationen, Banktransaktionen, …)
  - Dialer verursachen riesige Telefonrechnungen
- **Einbrecher** (**Hacker**)
  - Eindringen über Schwachstellen im Betriebssystem
  - oder über schon vorhandene trojanische Pferde in Rechner,
  - um dort vorhandene Daten auszuspähen
  - oder Rechner zu missbrauchen.
- Sie werden **beim Surfen ausspioniert und getäuscht**
  - Werbemails
  - Persönlichkeitsprofile
  - Phishing-Angriffe entlocken Ihnen vertraulicher Informationen

19

Viren, Würmer, Trojanische Pferde (1)

- **Installieren Sie Antiviren-Software!**
  - **Sammellizenzen** des Landes Niedersachsen und der Max-Planck-Gesellschaft
    - für alle dienstlich genutzten Rechnern
    - für nicht kommerziell genutzte Privatrechner
    - für alle Studierenden der Universität Göttingen
- **Halten Sie Ihre Antivirensoftware aktuell!**
  - Neue Schädlinge werden fast täglich in Umlauf gesetzt.
  - Nur ständig aktualisierte Antivirensoftware kann daher den nötigen Schutz bieten.
- Beschreibungen für die Installation und Aktualisierung
  - http://antivir.gwdg.de

20

Viren, Würmer, Trojanische Pferde (2)

- **Viren in Mails**
  - Viele Viren werden über Massenmails verteilt durch
    - **aktive Inhalte** von Mails und
    - **Mailanhänge**
  - Gehen Sie **vorsichtig mit Mailanhängen** um!
    - Öffnen Sie diese nur, wenn Sie sich über die Herkunft und den Inhalt im Klaren sind!
    - Absender solcher Mails könnten gefälscht sein – trauen Sie der Absenderadresse nicht!
  - Erlauben Sie **keine aktiven Inhalte** in Mails
  - **Mailserver können alle mit bekannten Viren behafteten Mails ausfiltern**.
    - Nutzen Sie den Mailserver der GWDG oder einen anderen Mailserver, der Sie vor Viren schützt!
    - Dieser Schutz ist nie vollständig
    - Immer wieder verbreiten sich Viren so schnell, dass die Antivirensoftware zeitweise nicht schützen kann

Viren, Würmer, Trojanische Pferde (3)

- **Würmer greifen über Netze direkt an**
  - Manche Würmer dringen über von Virenscannern nicht überwachte Schnittstellen in den Rechner ein.
    - Der Virenscanner schützt also nicht vor dem **Eindringen** der Würmer!
  - Lassen Sie den Virenscanner daher **regelmäßig die Festplatte nach Viren durchsuchen**!
  - Würmer lassen sich nur abwehren, wenn alle **Softwarekorrekturen** installiert werden
- **Gefahren beim Surfen**
  - **Nicht alle Internetseiten sind seriös**.
  - Wegen eines unsicher konfigurierten Browsers können Sie sich daher **Trojanische Pferde** und andere Schädlinge einhandeln.
  - Viele dieser Schädlinge kann ein **regelmäßiger Virenscan** finden.
  - Noch wichtiger ist, einen sicheren bzw. **sicher konfigurierten Browser** zu benutzen.
  - Hinweise dazu finden Sie unter http://www.gwdg.de/service/sicherheit
  - oder fragen Sie Ihren Administrator

A.9 Abmelden und ausschalten

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Bei kürzerem Verlassen des Zimmers muss der Arbeitsplatzrechner **durch einen Kennwortschutz gesperrt** werden.

Bei längerem Verlassen des Zimmers muss sich der Benutzer aus den laufenden Anwendungen und dem Betriebssystem **abmelden**.

Grundsätzlich sind die Systeme **nach Dienstschluss auszuschalten**.

Von diesen Regelungen kann nur **abgewichen** werden, soweit es die Arbeitsorganisation dringend erfordert und/oder andere Sicherheitsmaßnahmen es ermöglichen.

23

A.10 Personenbezogene Kennungen

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Alle Rechnersysteme sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist zunächst eine **Anmeldung mit Benutzerkennung und Passwort erforderlich**.

Die Vergabe von Benutzerkennungen für die Arbeit an IT-Systemen soll in der Regel **personenbezogen** erfolgen.

Die Arbeit unter der **Kennung einer anderen Person ist unzulässig**.

Dem Benutzer ist untersagt, Kennungen und Passwörter **weiterzugeben**.

Ausgenommen von dieser Regelung sind Systeme, die für allgemeine öffentliche Zugänge bestimmt sind (z.B. Kiosksysteme, Abfragestationen für Bibliothekskataloge).

24

GWDG

A.11 Gebrauch von Passwörtern

- **Verantwortlich für Initiierung: IT-Beauftragter**
  Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

  Der Benutzer hat sein Passwort geheim zu halten. Idealerweise sollte das Passwort nicht notiert werden.
  Für die Wahl von Passwörtern werden folgende Regeln dringend empfohlen:
  - Das Passwort muss mindestens 8 Stellen lang sein.
  - Das Passwort darf nicht leicht zu erraten sein wie Namen, Kfz-Kennzeichen, Geburtsdaten.
  - Das Passwort muss mindestens einen Groß- und Kleinbuchstaben und mindestens eine Ziffer und mindestens ein Sonderzeichen enthalten.
  - Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
  - Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
  - Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln und sollte eine Mindestgültigkeitsdauer von einem Tag haben.
  - Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.
  - Das Passwort sollte nur für die Hinterlegung schriftlich fixiert werden, wobei es dann in einem verschlossenen Umschlag sicher aufbewahrt wird. Wird es darüber hinaus aufgeschrieben, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.
  - Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.
  - Die Eingabe des Passwortes muss unbeobachtet stattfinden.

  Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt. Abweichungen von den oben genannten Regeln sollten in einer separaten Sicherheitsrichtlinie für Passwortschutz festgelegt werden.
  Erhält ein Benutzer beim Anmelden mit seinem Passwort keinen Zugriff auf das System, besteht die Gefahr, dass sein Passwort durch Ausprobieren ermittelt werden sollte, um illegal Zugang zum System zu erhalten. Solche Vorfälle sind dem zuständigen Vorgesetzten und dem IT-Personal zu melden (Siehe A.2).

  Vergisst ein Benutzer sein Passwort, hat er beim Administrator ohne vorheriges Ausprobieren das Zurücksetzen zu veranlassen. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird.

GWDG

Kennwörter

- Ein **leidiges Thema**
  - Leicht zu merkende Kennwörter sind auch leicht zu erraten.
  - Gute (komplexe) Kennwörter können leicht vergessen werden und kleben daher oftmals unter der Tastatur.
- **Probieren ist für Hacker oder Würmer einfach!**
  - Ein Computer kann tausende Kennwörter pro Sekunde ausprobieren.
- Regeln für ein gutes Kennwort
  - Mindestens 8 **Zeichen**
  - **Mischung** aus **Groß-** und **Kleinbuchstaben**, **Zahlen**, **Sonderzeichen**
  - **keine Namen oder Wörter** (Wörterbuch-Attacken!)
  - auch nicht umgekehrt oder permutiert oder mit einer Zahl dazu
  - Tipp: Anfangs- bzw. Endbuchstaben von einem Satz oder einem Motto:
    Ein gutes Kennwort – sollte man behalten können = 1gK-smbk
- Kennwörter **nie** im Betriebssystem oder einer Anwendung **abspeichern**
- Kennwörter **regelmäßig ändern**
- **Vorsicht vor Spionage** beim Eintippen
- Kennwörter **nicht weitergeben**

A.12 Zugriffsrechte

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Personal

Der Benutzer darf nur mit den **Zugriffsrechten ausgestattet werden, die unmittelbar für die Erledigung seiner Aufgaben** vorgesehen sind. Insbesondere sind alltägliche Arbeiten **nicht mit privilegierten Benutzerkonten (Administrator, root o.a.)** vorzunehmen.

Bei allen administrativen Anwendungen, die **gesetzlichen Anforderungen** genügen müssen (Datenschutz, Handelsgesetzbuch, u.a.) erfolgt die Vergabe bzw. Änderung der Zugriffsrechte für die einzelnen Benutzer auf schriftlichen Antrag.

Bei der Vergabe von Zugriffsrechten ist die **Funktionstrennung** zu beachten (Administratoren dürfen sich nicht selbst verwalten).

In allen anderen Bereichen sind die dort geltenden Regelungen zu beachten.

Sichere Konfiguration

- **Angriffsfläche minimieren**
  - Installieren Sie nur die benötigten Dienste!
    - keine unnötigen WWW-, FTP-, Telnet- usw. Server auf Arbeitsplatzrechnern
    - keine unnötigen Freigaben von Laufwerken und Druckern
- **Nicht mit Administrator-Rechten arbeiten**
  - Windows 9x/ME kennt keine unterschiedlichen Rechte!
- **Sichere Kennwörter**
- Konfigurieren Sie **Netzwerkanwendungen** sicher!
  - **Internetbrowser**
    - Aktive Inhalte nicht erlauben
    - Ausnahmen nur bei gut bekannten Anbietern
    - Problem der Bequemlichkeit
    - Cookies und Web-Bugs s.u.
  - **Mailprogramm**
    - Aktive Inhalte verbieten,
    - HTML-Mails in Text umwandeln lassen,
    - keine automatische Vorschau,
    - keine HTML-Mails verschicken,

A.13 Netzzugänge

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Der **Anschluss** von Systemen an das Datennetz der Universität Göttingen bzw. der Universitätsmedizin hat **ausschließlich über die dafür vorgesehene Infrastruktur** zu erfolgen.

Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Switches, Modems o. ä.) ist unzulässig.

Ausnahmen dürfen nur die zuständigen Rechenzentren in Absprache mit dem IT-Beauftragten des Bereichs und ggf. mit dem Datenschutzbeauftragten einrichten.

An das Datennetz dürfen nur die dafür vorgesehenen Systeme an den vorgesehenen Stellen angeschlossen werden.

29

A.14 Telearbeit

Verantwortlich für Initiierung: Bereichsleitung
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Bei der Telearbeit verlassen Daten den räumlich eingegrenzten Bereich der Daten verarbeitenden Stelle.

Zur Einrichtung und zum Betrieb von Telearbeitsplätzen ist eine Dienstvereinbarung erforderlich.

Dabei sind die Rahmenbedingungen jedes Einzelfalls zu berücksichtigen.

Der telearbeitende IT-Anwender hat die entsprechenden Vereinbarungen zum Schutz der bearbeiteten Daten und verwendeten System einzuhalten.

30

A.15 Sichere Netzwerknutzung

Verantwortlich für Initiierung: IT-Beauftragter
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Der Einsatz von **verschlüsselten Kommunikationsdiensten** ist, nach Möglichkeit, den unverschlüsselten Diensten vorzuziehen.

Die Übertragung schützenswerter Daten muss verschlüsselt erfolgen oder durch andere geeignete Maßnahmen (z.B. isolierter eigener Netze) gesichert werden.

31

A.16 Datensicherung

Verantwortlich für Initiierung: Verfahrensverantwortlicher
Verantwortlich für Umsetzung: IT-Personal

Regelmäßig durchgeführte Datensicherungen sollen vor Verlust durch Fehlbedienung, technische Störungen o. ä. schützen.

Grundsätzlich sind **Daten auf zentralen Servern zu speichern**.

Ist die Speicherung auf zentralen Servern noch nicht möglich, ist der **Benutzer für die Sicherung seiner Daten selbst verantwortlich**.

Bei zentraler Datensicherung sollte sich der **Nutzer** über die in den jeweiligen Bereichen geltenden Regelungen zu Rhythmus und Verfahrensweise für die Datensicherung **informieren**.

32

A.17 Umgang mit Datenträgern

Verantwortlich für Initiierung: Verfahrensverantwortlicher
Verantwortlich für Umsetzung: IT-Personal

Datenträger sind an **gesicherten Orten aufzubewahren**. Ggf. sind Datenträgertresore zu beschaffen.

Weiterhin sind Datenträger zu **kennzeichnen**, falls die Identifikation des Datenträgers nicht durch ein anderes technisches Verfahren erfolgt.

Datenträger müssen beim **Transport** vor Beschädigungen geschützt sein. Bei **schützenswerten Daten ist eine Verschlüsselung** erforderlich.

33

A.18 Physisches Löschen von Datenträgern

Verantwortlich für Initiierung: Verfahrensverantwortlicher
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Datenträger mit schützenswerten Daten müssen vor einer Weitergabe an nicht autorisierte Personen **physisch gelöscht** werden. Das kann mit geeigneten Programmen oder mit einem Gerät zum magnetischen Durchflutungslöschen erfolgen.

Auszusondernde oder defekte Datenträger müssen, sofern sie schützenswerte Daten enthalten (oder enthalten haben), vollständig unlesbar gemacht werden.

Weitere Informationen und Auskünfte zum Löschen von Datenträgern geben: **GWDG** (Helpdesk), **Geschäftsbereich Informationstechnologie** für die Universitätsmedizin (Servicecenter), die **Hotline der Stabstelle DV** für die Universitätsverwaltung, die **Datenschutzbeauftragten** der Universität und der Universitätsmedizin.

34

A.19 Schützenswerte Daten auf dem Arbeitsplatzrechner

Verantwortlich für Initiierung: Verfahrensverantwortlicher
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Das Speichern **schützenswerter Daten auf der Festplatte des Arbeitsplatzrechners oder anderer lokaler Speicher- oder Übertragungsmedien** und deren Übertragung ist nur zulässig, wenn die für den jeweiligen Schutzbedarf (die für die jeweilige Schutzstufe) **erforderlichen Sicherheitsmaßnahmen** getroffen wurden (s. z.B. § 9 Bundesdatenschutzgesetz, Grundschutzhandbuch des BSI, Hinweise des/der Datenschutzbeauftragten).

35

A.20 Sichere Entsorgung vertraulicher Papiere

Verantwortlich für Initiierung: Verfahrensverantwortlicher
Verantwortlich für Umsetzung: IT-Personal, IT-Anwender

Papiere mit vertraulichem Inhalt (auch Testausdrucke) sind mit Hilfe eines **Aktenvernichters** zu vernichten. Alternativ kann die Entsorgung auch zentral über einen Dienstleister erfolgen.

Bei der Entsorgung über einen Dienstleister sind die universitären Regelungen zu beachten.

36

Weitere Informationen

- **Universität Göttingen**
  - **Sicherheitsrichtlinien der Universität und Universitätsmedizin**
    - it-sicherheit.uni-goettingen.de
- **GWDG**
  - **Informationen über Sicherheitsthemen**
    - http://www.gwdg.de/index.php?id=66
  - **Installationshilfen** für einige Software-Produkte/Windows-Versionen
    - http://www.gwdg.de/index.php?id=1518
  - Mailingliste **GWDG-SEC**
    - Archiv unter https://listserv.gwdg.de/mailman/private/gwdg-sec
  - **Kursskripten** zu den Kursen in der GWDG
    - http://www.gwdg.de/index.php?id=192
  - **Allgemeines zu Sicherheit**
  - www.bsi-fuer-buerger.de/aktuell
  - www.allgemeiner-datenschutz.de
  - www.sicherheit-im-internet.de
- **Selbsttests**
  - http://www.heise.de/ct/browsercheck
  - http://check.lfd.niedersachsen.de/start.php
  - http://www.datenschutz.ch

- Danke für ihre Aufmerksamkeit

Fragen, Probleme, Anregungen?