### *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.

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

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

### *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.

### *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.

## Kommunikationssicherheit

### *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.

## Datensicherung

### *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.

## Datenträger

### *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.

### *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.

## Schützenswerte Daten

### *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).

### *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.

* Ein Hinweis zur Sprachregelung: Der Artikel »der«, »die« oder »das« ist bei Personenbezeichnungen und bei der Bezeichnung von Personengruppen nicht generell als Markierung des Geschlechts zu verstehen (Institut für deutsche Sprache, Mannheim). Sofern nicht ausdrücklich anders bezeichnet, ist stets die weibliche und die männliche Form gemeint.

Arbeitsgruppe IT-Sicherheit
Kontakt: agitsi@uni-goettingen.de
http://it-sicherheit.uni-goettingen.de
*Stand: Juni 2007*



GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

UNIVERSITÄTSMEDIZIN
GÖTTINGEN : UMG

# Maßnahmen des IT-Grundschutzes für IT-Anwender

Auszüge aus der
IT-Sicherheitsrahmenrichtlinie
der Universität Göttingen
und der Universitätsmedizin Göttingen

## Vorbemerkung

Das Sicherheitskonzept wendet sich an alle Mitarbeiter und Mitarbeiterinnen* sowie die Angehörigen der Universität und Universitätsmedizin Göttingen

## Allgemeines

### *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.

### *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.

### *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 erheblichem 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.

## Sicherung der Infrastruktur

### *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.

## Hard- und Software

### *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.

### *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.

### *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.

## Zugriffsschutz

### *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.

### *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).

### *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.