GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Datum: 15.06.2007 Nr.: 11

AMTLICHE.MITTEILUNGEN

Inhaltsverzeichnis

Herausgegeben vom Präsidenten der Georg-August-Universität Göttingen

Redaktion:
Abteilung Wissenschaftsrecht und Trägerstiftung

Goßlerstr. 5/7
37073 Göttingen

Telefon
+ 49 551/39-4496

e-mail: am-redaktion@zvw.uni-goettingen.de
Internet: www.uni-goettingen.de/de/sh/6800.html

Präsidium:

Das Präsidium der Georg-August-Universität Göttingen hat gemeinsam mit dem Vorstand der Universitätsmedizin Göttingen die nachfolgende Sicherheitsrahmenrichtlinie der Georg-August-Universität Göttingen und der Universitätsmedizin Göttingen beschlossen (§ 37 Abs. 1 Satz 3 1. Halbsatz NHG in der Fassung der Bekanntmachung vom 26.02.2007 (Nds. GVBl. S. 69); § 63 e Abs. 1 Satz 1 NHG).

Sicherheitsrahmenrichtlinie der Georg-August-Universität Göttingen und der Universitätsmedizin Göttingen

Inhaltsverzeichnis

1 Vorbemerkungen

Das Sicherheitskonzept wendet sich an alle Mitarbeiter und Mitarbeiterinnen sowie die Angehörigen der Universität und Universitätsmedizin Göttingen.[1]
Das Sicherheitskonzept besteht aus drei Teilen:

- einer Organisationsrichtlinie zur IT-Sicherheit, die die Strukturen des IT-Sicherheitsprozesses festlegt,
- dieser IT-Sicherheitsrahmenrichtlinie und
- ggf. Einzelrichtlinien für spezifische Maßnahmen insbesondere zur Konkretisierung der Prinzipien der Rahmenrichtlinien.

Das Sicherheitskonzept orientiert sich im Allgemeinen am Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI).
Ergänzungen und Erläuterungen zu dieser Rahmenrichtlinie werden im Netz unter http://it-sicherheit.uni-goettingen.de bereitgestellt.
Der Maßnahmenkatalog betrachtet Maßnahmen des Grundschutzes. Es wird dabei vorausgesetzt, dass in der Regel nur ein niedriger bis mittlerer Schutzbedarf besteht. Diese Annahme ist grundsätzlich für jedes IT-System und IT-Verfahren zu prüfen. Wird ein höherer Schutzbedarf festgestellt, so sind geeignete zusätzliche Maßnahmen zu ergreifen.
Nicht alle Maßnahmen sind immer umsetzbar. Ausnahmen sind prinzipiell erlaubt, wenn sie begründet, dokumentiert und von zuständiger Stelle (d.h. i.d.R. der Leitung der jeweiligen Organisationseinheit) genehmigt und damit auch verantwortet werden.

[1] 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.

2 Maßnahmen des IT-Grundschutzes für IT-Anwender

2.1 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 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.

2.2 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.

2.3 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 Studierendenarbeitsbereiche, und im Funknetz Goe-Mobile.

- **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.

2.4 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.

- **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 Systeme einzuhalten.

2.5 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.

2.6 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.

2.7 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.

2.8 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.

3 Maßnahmen des IT-Grundschutzes für IT-Personal

Die im Folgenden beschriebenen Maßnahmen richten sich an alle Mitarbeiter der Universität Göttingen, die verantwortlich Aufgaben im Bereich des IT-Betriebs wahrnehmen oder Verantwortung im organisatorischen Bereich tragen. Insbesondere sind dies IT-Abteilungsleiter, IT-Beauftragte, Verfahrensverantwortliche, System-, Netzadministratoren, Applikationsbetreuer, Benutzerservice, Programmentwickler u.a.. Die im vorangegangenen Abschnitt dargestellten Maßnahmen für den IT-Anwender werden hier vorausgesetzt.
Im Interesse einer möglichst übersichtlichen Darstellung werden einige Maßnahmen wiederholt, wobei sie gelegentlich weiter ausgeführt oder erweitert werden. Bei spezifischen Aufgabenstellungen, insbesondere im Umfeld von System- und Netzadministration, kann eine Abweichung in einzelnen Punkten der zuvor behandelten Maßnahmen notwendig sein. In jedem Fall ist aber der zugrunde liegende Sicherheitsgedanke nicht außer Kraft zu setzen, sondern der gegebenen Situation anzupassen.

3.1 Allgemeines

- **I.1 Verantwortung**

Verantwortlich für Initiierung:	AG „IT-Strategie“
Verantwortlich für Umsetzung:	Bereichsleitung

Die Verantwortung für die Umsetzung und Einhaltung der für den IT-Einsatz geltenden Regelungen tragen die einzelnen Leitungen der Einrichtungen entsprechend der Organisationsrichtlinie zur IT-Sicherheit der Universität.

- **I.2 Bekanntmachung von Richtlinien und Zuständigkeitsregelungen**

Verantwortlich für Initiierung:	AG „IT-Strategie“
Verantwortlich für Umsetzung:	Bereichsleitung

Die Organisationsrichtlinie zur IT-Sicherheit und die IT-Sicherheitsrahmenrichtlinie der Universität sind allen Beschäftigten der Universität bekannt zu machen. Die Kenntnisnahme ist durch die IT-Beauftragten schriftlich zu dokumentieren.

Bei Mitarbeitern, die vor Verabschiedung dieser Regelungen eingestellt wurden, ist die Bekanntmachung nachzuholen.

Mit zusätzlichen Richtlinien und Zuständigkeitsregelungen für einzelne Bereiche oder spezielle Verfahren sind alle betroffenen Mitarbeiter entsprechend zu informieren.

Über alle Änderungen an Richtlinien und Zuständigkeitsregelungen sind alle Beschäftigen umgehend zu informieren.

- **I.3 IT-Beauftragte**

Verantwortlich für Initiierung:	AG „IT-Strategie“
Verantwortlich für Umsetzung:	Bereichsleitung

Den IT-Beauftragten der Bereiche kommt im Rahmen des Sicherheitsrahmenkonzeptes der Universität Göttingen eine zentrale Bedeutung zu, denn sie haben in ihrem Zuständigkeitsbereich die für den IT-Einsatz gebotenen technischen und organisatorischen Maßnahmen zur IT-Sicherheit zu initiieren und zu koordinieren; sie führen die notwendigen Aufzeichnungen für den Bereich ihrer Zuständigkeit. Bei Fragen des IT-Einsatzes sind sie sowohl Ansprechpartner für die Mitarbeiter ihres Bereiches als auch für Dritte (Bereichsfremde).

3.2 Organisation von IT-Sicherheit

- **I.4 Frühzeitige Berücksichtigung von IT-Sicherheitsfragen**

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

Fragen der IT-Sicherheit sind bei Neubeschaffungen von IT-Systemen und der Einführung neuer Verfahren im Planungsstadium zu berücksichtigen.

- **I.5 Rollentrennung**

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

Für jedes IT-Verfahren sind die Verantwortlichkeiten für alle Bereiche eindeutig festzulegen. Normalerweise ist eine Rollentrennung von Verfahrensentwicklung/-pflege und Systemadministration sinnvoll. Jedem Mitarbeiter müssen die ihm übertragenen Verantwortlichkeiten und die ihn betreffenden Regelungen bekannt sein. Abgrenzungen und Schnittflächen der verschiedenen Anwenderrollen müssen klar definiert sein.

- **I.6 Dokumentation und Beschreibung der IT-Verfahren**

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

Es wird empfohlen, zur Gewährleistung der IT-Sicherheit eines Verfahrens eine Dokumentation und Beschreibung zu erstellen. Hierzu gehören u. a. folgende Angaben:

- Aufgabe des Verfahrens
- Systemübersicht, Netzplan
- Schnittstellen zu anderen Verfahren
- Datenbeschreibung

Es wird empfohlen, IT-Verfahren bezüglich der Sicherheit mindestens hinsichtlich der folgenden Punkte zu dokumentieren:

- Vertretungsregelungen, insbesondere im Administrationsbereich
- Zugriffsrechte
- Organisation, Verantwortlichkeit und Durchführung der Datensicherung
- Installation und Freigabe von Software
- Zweck, Freigabe und Einsatz selbst erstellter Programme
- Dienstanweisungen
- Arbeitsanleitungen für Administrationsaufgaben u.ä.
- auftretende Sicherheitsprobleme aller Art
- Notfallregelungen

- Wartungsvereinbarungen
- Verfahrensbeschreibungen nach Datenschutzrecht

Nur dokumentierte Verfahren dürfen betrieben werden. Der IT-Beauftragte sorgt für die aktuelle Dokumentation der Verfahren seines Bereiches. Der IT-Beauftragte ist verantwortlich für die Erstellung und Pflege der Dokumentation der Verfahren seines Bereiches. Verfahrensverantwortliche, Systemadministratoren und Applikationsbetreuer sind dabei zur Mitarbeit verpflichtet. Für Bereiche der technischen Infrastruktur sind ggf. die jeweiligen IT-Dienstleister für die Dokumentation der Verfahren verantwortlich.

- **I.7 Dokumentation von Ereignissen und Fehlern**

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

Ereignisse, die Indiz für ein Sicherheitsproblem sein können, können für die Fortschreibung der IT-Sicherheitsrahmenrichtlinie wertvolle Hinweise liefern. Sie sind daher zu dokumentieren. Zu dokumentieren sind Sicherheitsprobleme und -vorfälle, die aus Sicht des betroffenen Mitarbeiters für die übergreifende IT-Sicherheit von Bedeutung sein können. Der Mitarbeiter bzw. der zuständige IT- Beauftragte meldet die dokumentierten Vorfälle regelmäßig oder bei Bedarf sofort an die Arbeitsgruppe „IT-Sicherheit“.

- **I.8 Regelungen der Auftragsdatenverarbeitung**

Verantwortlich für Initiierung:	Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	Verfahrensverantwortlicher

Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag der Universität Göttingen betriebenen IT-Verfahren. Es sind eindeutige Zuweisungen der Verantwortlichkeit für die IT-Sicherheit zu schaffen und entsprechende Kontrollmöglichkeiten vorzusehen.

Sofern im Rahmen der Auftragsdatenverarbeitung personenbezogene Daten verarbeitet werden, sind die entsprechenden Regelungen des Niedersächsischen Datenschutzgesetzes (NDSG) bzw. des Bundesdatenschutzgesetzes (BDSG) zu beachten. Für Wartungsarbeiten stellen die Datenschutzgesetze (NDSG, BDSG) besondere Regelungen bereit, die anzuwenden sind.

- **I.9 Standards für technische Ausstattung**

Verantwortlich für Initiierung:	AG „IT-Strategie“
Verantwortlich für Umsetzung:	IT-Dienstleister

Zur Erreichung eines ausreichenden Sicherheitsniveaus für IT-Systeme sind Qualitätsstandards im Sinne dieses Konzepts von der AG „IT-Sicherheit“ in Zusammenarbeit mit den zentralen IT-Dienstleistern unter Maßgabe der durch die AG „IT-Strategie“ definierten Strategien festzulegen.

- **I.10 Bereitstellung zentralisierter Serviceleistungen**

Verantwortlich für Initiierung:	AG „IT-Strategie“
Verantwortlich für Umsetzung:	IT-Dienstleister

Ein leistungsfähiger Nutzerservice, zentral gesteuerte Datensicherungsmaßnahmen, die Möglichkeit der Ablage von Daten auf zentrale Fileserver sowie die Möglichkeit der Ausführung von Programmen auf Applikationsservern sind wesentliche Voraussetzungen für einen sicheren und reibungslosen IT-Einsatz zur Unterstützung der

täglichen Arbeitsprozesse. Entsprechende Dienste sind möglichst zentral anzubieten.

Die Softwareverteilung inkl. -installation und -inventarisierung sollte mit Unterstützung entsprechender Werkzeuge erfolgen. Maßnahmen zur Virenabwehr sind ebenfalls zu zentralisieren.

Beim Einsatz netzwerkweit operierender Installations- und Inventarisierungswerkzeuge sind besondere Maßnahmen zum Schutz vor Missbrauch zu ergreifen. Insbesondere müssen verbindliche Regelungen getroffen werden, die sicherstellen, dass die Werkzeuge ausschließlich für diesen Zweck eingesetzt werden. Dazu muss u. a. festgelegt sein, dass die Werkzeuge nur auf dafür bestimmten, besonders abgesicherten Arbeitsplätzen eingesetzt werden. Der Personenkreis, der berechtigt ist, diese Werkzeuge zu nutzen, ist auf das notwendige Maß zu beschränken. Die Anwender sind vor dem Einsatz solcher Werkzeuge zu informieren. Ihr Einsatz muss protokolliert und dokumentiert werden.

- **I.11 Nutzung zentralisierter Serviceleistungen**

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

Ein leistungsfähiger Nutzerservice, zentral gesteuerte Datensicherungsmaßnahmen, die Möglichkeit der Ablage von Daten auf zentrale Fileserver sowie die Möglichkeit der Ausführung von Programmen auf Applikationsservern sind wesentliche Voraussetzungen für einen sicheren und reibungslosen IT-Einsatz zur Unterstützung der täglichen Arbeitsprozesse.

Durch die Bereitstellung wesentlicher IT-Dienste durch die zentralen IT-Dienstleister werden die Einrichtungen der Universität entlastet, um die eigentlichen Aufgaben besser erfüllen zu können. Durch eine Zentralisierung von IT-Dienstleistungen wird eine höhere Professionalität und damit verbesserte IT-Sicherheit erreicht.

Die Einrichtungen der Universität sollten eigene IT-Systeme nur soweit betreiben, wie dies für die eigenen Aufgabenstellungen notwendig ist und nach Möglichkeit auf zentrale Serviceleistungen der zentralen IT-Dienstleister zurückgreifen.

3.3 Personelle Maßnahmen

- **I.12 Vertretung**

Verantwortlich für Initiierung:	Bereichsleitung/Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	Bereichsleitung

Für alle Betreuungs- und Administrationsfunktionen sind Vertretungsregelungen erforderlich. Die Vertreter müssen alle notwendigen Tätigkeiten ausreichend beherrschen und ggf. auf schriftliche Arbeitsanweisungen und Dokumentationen zurückgreifen können. Die Vertretungsregelung muss im System abgebildet sein und darf nicht durch die Weitergabe von Passwörtern erfolgen.

Vertretungsrechte sollten im System möglichst ständig eingerichtet sein. Eine Ausnahme bilden systemspezifische, nicht nutzerabhängige Kennungen (zum Beispiel root bei UNIX-Systemen). Dort soll der Vertreter nur im Bedarfsfall auf das an geeigneter Stelle hinterlegte Passwort des Administrators zurückgreifen können.

Bei der Auswahl der Vertreter ist zu beachten, dass die Rollentrennung nicht unterlaufen wird.

- **I.13 Qualifizierung**

Verantwortlich für Initiierung:	Bereichsleitung / Verfahrensverantwortlicher
Verantwortlich für Umsetzung:	Bereichsleitung

IT-Personal darf erst nach ausreichender Schulung mit IT-Verfahren arbeiten. Dabei sind ihnen die für sie geltenden Sicherheitsmaßnahmen, die rechtlichen Rahmenbedingungen sowie ggf. die Erfordernisse des Datenschutzes zu erläutern. Es muss sichergestellt sein, dass die ständige Fortbildung des IT-Personals in allen ihr Aufgabengebiet betreffenden Belangen erfolgt.

3.4 Sicherung der Infrastruktur

- **I.14 Basismaßnahmen**

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

Zur Sicherung der IT-Infrastruktur ist eine Vielzahl baulicher und technischer Vorgaben zu beachten. Die technischen Maßnahmen zur Infrastruktur sind im Grundschutzhandbuch des BSI beschrieben. Die Zuständigkeit für Brandschutz und weiterer Sicherheitsinfrastruktur liegt bei der Feuerwehr bzw. der Stabsstelle Sicherheitswesen der Universität. Folgende Maßnahmen zur Sicherung der IT-Infrastruktur sind zu beachten:

- USV
- Brandschutz
- Schutz vor Wasserschäden
- Geschützte Kabelverlegung

- **I.15 Sicherung der Serverräume**

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

Alle Rechnersysteme mit typischer Serverfunktion, einschließlich der Peripheriegeräte (Konsolen, externe Platten, Laufwerke u. ä.), sind in separaten, besonders gesicherten Räumen aufzustellen. Der Zugang Unbefugter zu diesen Räumen muss zuverlässig verhindert werden. Je nach der Schutzbedürftigkeit sowie in Abhängigkeit von äußeren Bedingungen (öffentlicher zugänglicher Bereich, Lage zur Straße usw.) sind besondere bauliche Maßnahmen, wie zum Beispiel einbruchsichere Fenster, einbruchsichere Türen, Bewegungsmelder o. ä. zur Verhinderung von gewaltsamen Eindringen vorzusehen. Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; verwendete Schlüssel müssen kopiergeschützt sein.

Für die Schlüsselverwaltung sind besondere Regelungen erforderlich, die eine Herausgabe an Unbefugte ausschließen. Der Zutritt muss auf diejenigen Personen begrenzt werden, deren Arbeitsaufgaben dieses erfordert.

Es ist zu prüfen, welche Serverräume Reinigungs- und Servicepersonal nur unter Aufsicht betreten darf.

- **I.16 Geschützte Aufstellung von Endgeräten**

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

Der unbefugte Zugang zu Geräten und die Benutzung der IT muss verhindert werden. Bei Abwesenheit des IT-Personals sind Räume mit IT verschlossen zu halten. Es muss gewährleistet sein, dass Schlüssel und Zugangsrechte nur an die jeweils berechtigten Personen ausgegeben werden. Bei der Anordnung und Einrichtung der Geräte ist darauf zu achten, dass Daten mit internen oder vertraulichen Inhalt nicht von Unbefugten eingesehen werden können. Beim Ausdrucken derartiger Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden.

- **I.17 Sicherung der Netzknoten**

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

Vernetzungsinfrastruktur (Switches, Router, Hubs, Wiring-Center u. ä.) ist grundsätzlich in verschlossenen Räumen oder in nicht öffentlich zugänglichen Bereichen in verschlossenen Schränken einzurichten, die gegen unbefugten Zutritt und Zerstörung ausreichend gesichert sind. Es gelten die gleichen Empfehlungen wie unter I.15 Sicherung der Serverräume.

- **I.18 Verkabelung und Funknetze**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	IT-Dienstleister

Die Verkabelung des LAN ist klar zu strukturieren sowie aktuell und vollständig zu dokumentieren. Die Administratoren müssen einen vollständigen Überblick über die Kabelverlegung und die Anschlussbelegung zentraler Komponenten haben.

Nicht benutzte Anschlüsse sollen abgeklemmt oder deaktiviert werden.

Erweiterungen und Veränderungen an der Gebäudeverkabelung, auch die Inbetriebnahme von Funknetzen, sind mit den IT-Beauftragten des eigenen Bereichs und mit den zuständigen zentralen Stellen (GWDG bzw. GB-IT als Rechenzentren, Gebäudemanagement, AG „IT-Sicherheit“) abzustimmen.

- **I.19 Einweisung und Beaufsichtigung von Fremdpersonal**

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

Fremde Personen, die in gesicherten Räumen mit IT (z.B. Serverräume) Arbeiten auszuführen haben, müssen beaufsichtigt werden. Personen, die nicht unmittelbar zum IT-Bereich zu zählen sind, aber Zugang zu gesicherten IT-Räumen benötigen, müssen über den Umgang mit IT belehrt werden.

Wenn bei Arbeiten durch externe Firmen, zum Beispiel im Rahmen der Fernwartung, die Möglichkeit des Zugriffs auf personenbezogene Daten besteht, müssen diese Personen gemäß § 5 des Niedersächsischen Datenschutzgesetzes (NDSG) bzw. § 5 des Bundesdatenschutzgesetzes (BDSG) verpflichtet sein. Für die Wartung und Instandhaltung sind Verträge gemäß § 6 NDSG bzw. § 11 BDSG zu schließen.

Alle Aktionen, die von externen Firmen durchgeführt werden, sollten nach Möglichkeit überwacht und protokolliert werden.

3.5 Hard- und Softwareeinsatz

- **I.20 Beschaffung, Softwareentwicklung**

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

Die Beschaffung von Soft- und Hardware ist mit dem zuständigen IT-Beauftragten abzustimmen. Dieser ist für die Einhaltung von Standards und Sicherheitsanforderungen verantwortlich.

Bei der Entwicklung von Software müssen vorher die fachlichen und technischen Anforderungen spezifiziert sein. Diese Arbeiten werden in enger Abstimmung mit den betroffenen Bereichen durchgeführt.

- **I.21 Kontrollierter Softwareeinsatz**

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

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. Ggf. steht die AG „IT-Sicherheit“ der Leitung beratend zur Seite.

- **I.22 Separate Entwicklungsumgebung**

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

Die Entwicklung oder Anpassung von insbesondere serverbasierter Software darf nicht in der Produktionsumgebung erfolgen. Die Überführung der Software von der Entwicklung in den Produktionsbetrieb bedarf der Freigabe durch den zuständigen IT-Beauftragten.

- **I.23 Schutz vor Schadprogrammen**

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

Auf allen Arbeitsplatzrechnern ist, soweit möglich, ein aktueller Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Jeder Bereich ist verpflichtet, Virenschutzsysteme anzubieten. Durch den Einsatz von Virenschutzsystemen soll das Eindringen von schädlichem Programmcode erkannt und verhindert werden. Regelmäßig (möglichst automatisiert) sind die Virenerkennungsmuster zu aktualisieren. Wird auf einem System schädlicher Programmcode entdeckt, muss dies der zuständigen Stelle gemeldet und das Ergebnis der eingeleiteten Maßnahmen dokumentiert werden.

Empfehlenswert ist, in regelmäßigen Abständen sowie bei konkretem Bedarf oder Verdacht eine Suche nach Schadprogrammen auf allen bedrohten IT-Systemen vorzunehmen und die Ergebnisse zu dokumentieren.

Von Herstellern bereitgestellte Softwareaktualisierungen zur Beseitigung von Sicherheitslücken sind nach geeigneten Tests zeitnah einzuspielen.

Anwendungen – insbesondere Netzanwendungen wie Mailprogramme und WWW-Browser – sind sicher zu konfigurieren, so dass Schadprogramme nicht unnötig leicht aktiv werden können. Um Angriffsflächen zu minimieren, darf nur benötigte Software installiert werden.

Anwendungen sind - soweit technisch - möglich ohne besondere Privilegien im Betriebssystem (Administratorrechte) auszuführen.

- **I.24 Diskettenlose PCs**

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

Bei erhöhtem Schutzbedarf müssen alle äußeren Zugänge des PCs (zum Beispiel Disketten- und CD-ROM-Laufwerke, USB-Anschlüsse, Wechseldatenträger) gesperrt werden, wenn sie für die zu erledigenden Aufgaben nicht notwendig sind. Die Möglichkeit der Nutzung von Applikationsservern und laufwerkslosen Arbeitsplatzrechnern bzw. Terminals ist zu prüfen. Der Zugriff auf das Rechner-BIOS ist durch ein Passwort zu schützen.

- **I.25 Ausfallsicherheit**

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

Maßnahmen zur Ausfallsicherheit sind entsprechend der jeweiligen Anforderung zu ergreifen. IT-Systeme, die zur Aufrechterhaltung eines geordneten Betriebs notwendig sind, müssen durch Ausweichlösungen (redundante Geräteauslegung oder Übernahme durch gleichartige Geräte mit leicht verminderter Leistung) oder Wartungsverträge mit kurzen Reaktionszeiten hinreichend verfügbar gehalten werden.

- **I.26 Einsatz von Diebstahl-Sicherungen**

Verantwortlich für Initiierung:	IT-Beauftragter
Verantwortlich für Umsetzung:	Technische Abteilung, IT-Personal

Diebstahl-Sicherungen sind überall dort einzusetzen, wo große Werte zu schützen sind bzw. dort, wo andere Maßnahmen – z. B. geeignete Zutrittskontrolle zu den Arbeitsplätzen – nicht umgesetzt werden können. Diebstahl-Sicherungen machen z. B. dort Sinn, wo Publikumsverkehr herrscht oder die Fluktuation von Benutzern sehr hoch ist. Mit Diebstahl-Sicherungen sollten je nach zu schützendem Objekt nicht nur das IT-System selber, sondern auch Monitor, Tastatur und anderes Zubehör ausgestattet werden.

Große Werte stellen auch Forschungsdaten und personenbezogene Daten dar. Datenträger mit solchen Daten sind deshalb in angemessener Weise zu schützen.

3.6 Zugriffsschutz

Grundsätzlich gilt, dass nur die Personen Zugang zu dem Netz und die damit verfügbaren Ressourcen der Universität Göttingen erhalten, die zuvor die Erlaubnis zur Nutzung von den dafür zuständigen Stellen erhalten haben. Jede Nutzungserlaubnis muss personengebunden sein, d.h. anonyme Nutzerkonten sollten nur in begründeten Ausnahmefällen (beispielsweise als Zugang für FTP- oder WWW-Server, organisatorische Anforderungen) erlaubt werden. Die Verwendung fremder Nutzerkennungen ist nicht erlaubt.
In der Regel ist der Zugang zum Netz verbunden mit dem Zugriff auf Daten, Anwendungsprogramme und weitere Ressourcen. Daher hat die Authentisierung der Nutzer des Netzes an jedem einzelnen Arbeitsplatzrechner der Universität eine besondere Bedeutung.

- **I.27 Netzzugänge**

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

Der Anschluss von Systemen an das Datennetz der Universität Göttingen hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige Einrichtung oder Benutzung von zusätzlichen Verbindungen (Modems o.ä.) ohne Absprache mit dem IT-Beauftragten des Bereichs und ggf. mit dem Datenschutzbeauftragten ist unzulässig. Die Netzbetriebsordnung der Universitätsmedizin und die Nutzungsbedingungen für Zugänge zum Internet über Anschlüsse der GWDG sind zu beachten.

- **I.28 Personenbezogene Kennungen (Authentisierung)**

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

Alle IT-Systeme und Anwendungen sind so einzurichten, dass nur berechtigte Benutzer die Möglichkeit haben, mit ihnen zu arbeiten. Infolgedessen ist 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.

Redundanzen bei der Benutzerverwaltung sind zu vermeiden. Die Zuordnung von mehreren Kennungen zu einer Person innerhalb eines IT-Systems sollte nur in begründeten Ausnahmefällen erlaubt sein, wie beispielsweise für Systemadministratoren. Die Einrichtung und Freigabe einer Benutzerkennung dürfen nur in einem geregelten Verfahren erfolgen. Die Einrichtung und Freigabe sind zu dokumentieren.

- **I.29 Administratorkennungen**

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

Das Verwenden von Benutzerkennungen mit weit reichenden Administrationsrechten muss auf die dafür notwendigen Aufgaben beschränkt bleiben. Die Administratoren erhalten für diese Aufgaben eine persönliche Administratorkennung. Für die alltägliche Arbeit sind Standard-Benutzerkennungen zu verwenden. Administrator-Konten sind nach Möglichkeit umzubenennen, damit deren Bedeutung nicht sofort ersichtlich ist.

- **I.30 Ausscheiden von Mitarbeitern**

Verantwortlich für Initiierung:	Bereichsleitung
Verantwortlich für Umsetzung:	Bereichsleitung, Vorgesetzter des ausscheidenden Mitarbeiters

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass der zuständige IT-Beauftragte rechtzeitig über das Ausscheiden oder den Wechsel eines Mitarbeiters informiert wird. Der zuständige Bereich des betreffenden Mitarbeiters hat über die Verwendung der dienstlichen Daten zu entscheiden, die der Kennung des ausscheidenden Mitarbeiters zugeordnet sind. Vor dem Ausscheiden sind sämtliche Unterlagen, die sicherheitsrelevante Angaben enthalten, ausgehändigte Schlüssel zurück zu fordern. Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt, so ist nach dem Ausscheiden einer der Personen die Zugangsberechtigung zu ändern.

- **I.31 Passwörter**

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

Werden in einem IT-System Passwörter zur Authentisierung gebraucht, so ist die Sicherheit der Zugangs- und Zugriffsrechteverwaltung des Systems entscheidend davon abhängig, dass das Passwort korrekt gebraucht wird. 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 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.
- Das Passwort sollte mindestens 8 Zeichen lang sein. Es muss getestet werden, wie viele Stellen des Passwortes vom Rechner überprüft werden.
- Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen durch individuelle Passwörter ersetzt werden.
- Passwörter dürfen nicht auf programmierbaren Funktionstasten gespeichert werden.
- Das Passwort muss geheim gehalten werden und sollte nur dem Benutzer persönlich bekannt sein.
- 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.
- Das Passwort ist regelmäßig, spätestens nach 360 Tagen, zu wechseln und sollte eine Mindestgültigkeitsdauer von einem Tag haben.
- Ein Passwortwechsel ist durchzuführen, wenn das Passwort unautorisierten Personen bekannt geworden ist.

- Alte Passwörter dürfen nach einem Passwortwechsel nicht mehr gebraucht werden.
- Die Eingabe des Passwortes muss unbeobachtet stattfinden.

Falls technisch möglich, sollten folgende Randbedingungen eingehalten werden:

- Die Wahl von Trivialpasswörtern ("BBBBBB", "123456") sollte verhindert werden.
- Jeder Benutzer muss sein eigenes Passwort jederzeit ändern können.
- Für die Erstanmeldung neuer Benutzer sollten Einmalpasswörter vergeben werden, also Passwörter, die nach einmaligem Gebrauch gewechselt werden müssen. In Netzen, in denen Passwörter unverschlüsselt übertragen werden, empfiehlt sich die dauerhafte Verwendung von Einmalpasswörtern.
- Nach dreifacher fehlerhafter Passworteingabe muss eine Sperrung erfolgen, die nur vom Systemadministrator aufgehoben werden kann.
- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nicht unverschlüsselt übertragen werden.
- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.
- Die Passwörter sollten im System zugriffssicher gespeichert werden, z. B. mittels Einwegverschlüsselung.
- Der Passwortwechsel sollte vom System regelmäßig initiiert werden.
- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).

Auf die Einhaltung der Regeln ist insbesondere zu achten, wenn das System diese nicht erzwingt.

• I.32 Zugriffsrechte (Autorisierung)

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

Über Zugriffsrechte wird geregelt, welche Person im Rahmen ihrer Funktionen bevollmächtigt wird, IT-Systeme, IT-Anwendungen oder Daten zu nutzen. Der Benutzer darf nur mit den Zugriffsrechten arbeiten, die unmittelbar für die Erledigung seiner Aufgaben vorgesehen sind.

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

Es ist zu prüfen, inwieweit die Zugriffserlaubnis auf bestimmte Arbeitsplatzrechner begrenzt werden kann. Für Benutzer mit besonderen Rechten, insbesondere für Administratorkennungen, ist eine Zugangsbegrenzung auf die notwendigen Rechner (i.d.R. sind es der betreffende Server und die Arbeitsplatzrechner) zu begrenzen. Es ist ebenfalls zu prüfen, inwieweit die Zugangserlaubnis auf bestimmte Zeiten begrenzt werden kann. Beispielsweise könnte der Zugang zu wichtigen Systemen für die Anwender auf die üblichen Arbeitszeiten eingeschränkt werden.

- **I.33 Änderung der Zugriffsrechte**

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

Im organisatorischen Ablauf muss zuverlässig verankert sein, dass das zuständige IT-Personal über die notwendige Änderung der Berechtigungen eines Anwenders, z. B. in Folge von Änderungen seiner Aufgaben, rechtzeitig informiert wird, um die Berechtigungsänderungen im System abzubilden.

- **I.34 Abmelden und ausschalten**

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

Bei kürzerem Verlassen des Raumes muss der Zugriff auf das IT-System durch einen Kennwortschutz gesperrt werden. Bei längerem Verlassen des Raumes sollte sich der Benutzer aus den laufenden Anwendungen und dem Betriebssystem abmelden. Grundsätzlich sind Arbeitsplatzrechner nach Dienstschluss auszuschalten, es sei denn, betriebliche Anforderungen sprechen dagegen. Soweit es technisch möglich ist, sollte jeder Rechner so konfiguriert sein, dass nach längerer Inaktivität (beispielsweise 10 Minuten) der PC automatisch gesperrt wird und nur nach erneuter Eingabe eines Passwortes zu aktivieren ist.

- **I.35 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. Durch entsprechende technische Maßnahmen ist sicherzustellen, dass

- bei der Kommunikation zwischen Telearbeitsplatz und Dienststelle die Vertraulichkeit und die Integrität der übertragenen Daten gewährleistet sind,
- nur Berechtigte von zu Hause aus auf dienstliche Daten zugreifen können,
- dienstliche Unterlagen am Telearbeitsplatz vertraulich behandelt werden und
- das gesamte Verfahren der Telearbeit revisionssicher ist.

Zur Einrichtung und zum Betrieb von Telearbeitsplätzen ist eine Dienstvereinbarung erforderlich. Weiterhin ist mit jedem Telearbeitnehmer ein Einzelvertrag zu schließen, der die spezifischen Rahmenbedingungen des jeweiligen Einzelfalls berücksichtigt. Werden bei der Telearbeit personenbezogene Daten verarbeitet, muss der zuständige Datenschutzbeauftragte am Genehmigungsprozess beteiligt werden.

3.7 System- und Netzwerkmanagement

Eine angemessene Protokollierung, Auditierung und Revision sind wesentliche Faktoren der Netzsicherheit. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss, ob die Bandbreite des Netzes den derzeitigen Anforderungen genügt oder systematische Angriffe auf das Netz zu erkennen sind.
Je nach Einsatz eines IT-Verfahrens müssen adäquate Maßnamen zur Protokollierung getroffen werden, um Datensicherheit, Datenschutz und Revisionsfähigkeit zu gewährleisten. Die Auswertung von Protokolldateien ist in Abhängigkeit mit den protokollierten Daten mit den Datenschutzbeauftragten, dem Personalrat und der Internen Revision abzustimmen.

- **I.36 Protokollierung auf den Servern**

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

Je nach den Möglichkeiten des Betriebssystems sind alle Zugangsversuche, sowohl die erfolgreichen als auch die erfolglosen, automatisch zu protokollieren. Das Ändern wichtiger Systemparameter und auch das Herunterfahren bzw. das Hochfahren des Systems sollten ebenfalls protokolliert werden.

Die Protokolle sollten regelmäßig und zeitnah ausgewertet werden. Es muss dabei sicher gestellt sein, dass nur die Personen Zugriff auf die Protokolle erlangen können, die dafür von der zuständigen Stelle mit den nötigen Rechten ausgestattet wurde. Das Prinzip der Zweckbindung nach § 10 Abs. 4 NDSG bzw. § 31 BDSG ist unbedingt zu beachten.

- **I.37 Protokollierung durch Anwendungsprogramme**

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

Bei der Protokollierung durch Anwendungssysteme ist der Grundsatz der Datenvermeidung nach § 3a BDSG zu beachten, d. h. die von Anwendungssystemen erzeugten Protokolldaten, die so wenig wie möglich personenbezogene Daten enthalten, sind vor dem Zugriff Unbefugter zu schützen. Es gelten die oben genannten Regeln entsprechend, insbesondere ist bei Daten mit Personenbezug das Zweckbindungsgebot zu beachten.

- **I.38 Protokollierung der Administrationstätigkeit**

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

Die Administratoren sind durch organisatorische Regelungen (Dienstanweisungen o.ä.) je nach Schutzbedarf des Verfahrens bzw. der zu verarbeitenden Daten zu verpflichten, die im Rahmen ihrer Aufgaben durchgeführten Tätigkeiten zu protokollieren.

3.8 Kommunikationssicherheit

Die gesamte elektronische Kommunikation der Universität wird durch eine Sicherheitsinfrastruktur in angemessener Weise geschützt. Besonderes Augenmerk gilt dabei der Kommunikation zwischen Bereichen mit unterschiedlichem Schutzbedarf.

Alle IT-Nutzer der Universität sind über die besonderen Risken und Gefahren der elektronischen Kommunikation und der Datenübermittlung in Kenntnis zu setzen.

- **I.39 Sichere Netzwerkadministration**

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

Es muss geregelt und sichergestellt sein, dass die Administration des lokalen Netzwerks nur von dem dafür vorgesehenen Personal durchgeführt wird. Aktive und passive Netzkomponenten sowie Server sind vor dem Zugriff Unbefugter zu schützen.

Die Netzdokumentation ist verschlossen zu halten und vor dem Zugriff Unbefugter zu schützen.

- **I.40 Netzmonitoring**

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

Es müssen geeignete Maßnahmen getroffen werden um Überlastungen und Störungen im Netzwerk frühzeitig zu erkennen und zu lokalisieren.

Es muss geregelt und sichergestellt sein, dass auf die für diesen Zweck eingesetzten Werkzeuge nur die dazu befugten Personen zugreifen können. Der Kreis der befugten Personen ist auf das notwendige Maß zu beschränken.

- **I.41 Deaktivierung nicht benötigter Netzwerkzugänge**

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

Es sind alle nicht benötigten Netzwerkzugänge zu deaktivieren, damit ein unbefugter Zugang zum Netz der Universität Göttingen verhindert wird.

- **I.42 Aufteilungen in Bereiche unterschiedlichen Schutzbedarfs**

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

Das Datennetz ist so zu strukturieren, dass Teilnetze für verschiedene IT-Systeme entsprechend ihres jeweiligen Schutzbedarfs bereitgestellt werden. Systeme mit unterschiedlichem Schutzbedarf sollten nicht in gleichen Teilnetzen betrieben werden. Dadurch wird verhindert, dass Systeme mit hohem Schutzbedarf durch zu wenig gesicherte Systeme im gleichen Teilnetz oder ungenügenden Schutzmaßnahmen an Netzübergängen gefährdet werden. Umgekehrt wird damit aber auch erreicht, dass die Nutzung von Systemen mit geringerem Schutzbedarf nicht unnötig erschwert wird, weil auf andere Systeme mit höherem Schutzbedarf im gleichen Teilnetz Rücksicht genommen werden muss.

- **I.43 Kontrollierte Kommunikationskanäle**

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

Die gesamte Kommunikation zwischen verschiedenen Teilbereichen oder mit externen Partnern darf ausschließlich über kontrollierte Kanäle erfolgen, die durch ein spezielles Schutzsystem (Firewall o.ä.) geführt werden. Die Regeln der Schutzsysteme sollten so definiert werden, dass unnötige Kommunikationen unterbunden werden und somit Angriffsflächen minimiert werden.

Die Installation und der Betrieb anderer Kommunikationsverbindungen neben den Netzverbindungen der Universität sind nicht gestattet. Falls auf Grund besonderer Umstände die Installation anderer Kommunikationswege unumgänglich ist (z.B. der Betrieb eines Modems zu Fernwartungszwecken), muss dies zuvor durch die zuständige Stelle genehmigt werden. Jeder Zugriff Externer ist zu protokollieren.

3.9 Datensicherung

- **I.44 Organisation der Datensicherung**

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

Die Datensicherung muss nach einem dokumentierten Datensicherungskonzept erfolgen, das dem Schutzbedarf der zu sichernden Daten angemessen ist. Es muss auch darüber Auskunft geben, nach welchen Kriterien die Datensicherung der Daten erfolgt. Im Falle personenbezogener Daten sind die geforderten Mindest- bzw. Höchstzeiträume zu beachten.

Das Datensicherungskonzept umfasst alle Regelungen der Datensicherung (was wird von wem nach welcher Methode, wann, wie oft und wo gesichert). Ebenso ist die Aufbewahrung der Sicherungsmedien zu regeln. Alle Sicherungen und das Aufbewahren von Sicherungsmedien sind zu dokumentieren (Datum, Art der Durchführung der Sicherung/gewählte Parameter, Beschriftung der Datenträger, Ort der Aufbewahrung).

- **I.45 Anwenderinformation zur Datensicherung**

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

Alle Anwender, die prinzipiell Datensicherungssysteme nutzen können, sollten über die Regelung zur Datensicherung informiert sein, um ggf. auf Unzulänglichkeiten (z.B. ungeeignetes Zeitintervall für ihren Bedarf) hinzuweisen oder individuelle Ergänzungen vornehmen zu können.

- **I.46 Durchführung der Datensicherung**

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

Vorzugsweise sollten Daten auf zentralen Fileservern gespeichert werden. Dort erfolgt turnusmäßig eine zentrale Datensicherung. Wo ein Zugriff auf einen Fileserver derzeit noch nicht möglich ist, müssen die Daten lokal gesichert werden.

Für Daten, deren Wiederherstellung mehr als einige Tage erfordert, sind mindestens 3 Generationen von Sicherungen vorzuhalten. Es ist empfehlenswert jeweils eine Sicherung für mindestens 3 bis 6 Monate aufzubewahren.

- **I.47 Durchführung der Datensicherung auf Servern**

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

Die Sicherung der Daten auf Servern sollte im angemessen Rhythmus erfolgen. Auch System- und Programmdaten sind nach Veränderungen zu sichern. Zur Datensicherung sind dafür geeignete Backup-Werkzeuge zu verwenden, die eine Datensicherung für Daten, deren Wiederherstellung mehr als einige Tage erfordert, nach dem Generationenprinzip unterstützt.

Nach Möglichkeit sind die Konfigurationen aller aktiven Netzkomponenten in eine regelmäßige Datensicherung einzubeziehen.

- **I.48 Verifizierung der Datensicherung**

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

Die Konsistenz der Datensicherungsläufe ist sicher zu stellen, d.h. die Lesbarkeit der Datensicherung ist zu überprüfen. Das testweise Wiedereinspielen von Datensicherungen soll wenigstens einmal jährlich erfolgen.

3.10 Datenträger

- **I.49 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.

- **I.50 Physikalisches Löschen und Entsorgen 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.

Die Reparatur beschädigter Datenträger, auf denen schützenswerte Daten gespeichert sind, ist nur in besonderen Ausnahmenfällen erlaubt. Wenn unter besonderen Umständen Datenträger durch externe Dienstleister repariert werden sollen, ist der Auftragnehmer auf die Wahrung der Vertraulichkeit der Daten zu verpflichten. Die Verpflichtung muss vertraglich verankert sein.

- **I.51 Sichere Entsorgung vertraulicher Papiere**

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

Papiere mit vertraulichem Inhalt sind mit Hilfe eines Aktenvernichters zu vernichten. Bei der Beschaffung eines Aktenvernichters ist die DIN 32757 zu beachten. Alternativ kann die Entsorgung auch über einen Dienstleister erfolgen. In diesem Fall muss sichergestellt sein, dass der Auftragnehmer über entsprechende Zertifikate verfügt. Der Auftragnehmer ist zur Protokollierung der Aktenvernichtung zu verpflichten.

Inkrafttreten

Diese Richtlinie wird vom Präsidium der Universität und vom Vorstand der Universitätsmedizin verabschiedet. Sie tritt am Tag nach ihrer Bekanntmachung in den Amtlichen Mitteilungen der Universität in Kraft.

Göttingen, 31. JAN. 2007

Für die Georg-August-Universität Göttingen
(ohne Universitätsmedizin)
- Der Präsident -

Prof. Dr. Kurt von Figura

Göttingen, 27. MRZ. 2007

Für die Universitätsmedizin Göttingen
- Der Sprecher des Vorstands -

Prof. Dr. Cornelius Frömmel

4 Anhang

Checklisten

Diese Checkliste ist dem „Leitfaden IT-Sicherheit“ des Bundesamts für Sicherheit in der Informationstechnik entnommen und soll den IT-Beauftragten und dem IT-Personal helfen einen schnellen Überblick über die Schwachstellen im IT-System der Universität zu erhalten.

IT-Sicherheitsmanagement	
❒	Hat die Unternehmens- bzw. Behördenleitung die IT-Sicherheitsziele festgelegt und sich zu ihrer Verantwortung für die IT-Sicherheit bekannt? Sind alle gesetzlichen oder vertragsrechtlichen Gesichtspunkte berücksichtigt worden?
❒	Gibt es einen IT-Sicherheitsbeauftragten?
❒	Werden IT-Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?
❒	Besteht ein Überblick über die wichtigsten Anwendungen und IT-Systeme und deren Schutzbedarf?
❒	Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen IT-Sicherheitsmaßnahmen regelt?
❒	Ist bei allen IT-Sicherheitsmaßnahmen festgelegt, ob sie einmalig oder in regelmäßigen Intervallen ausgeführt werden müssen (z. B. Update des Viren-Schutzprogramms)?
❒	Sind für alle IT-Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt?
❒	Gibt es geeignete Vertretungsregelungen für Verantwortliche und sind die Vertreter mit ihren Aufgaben vertraut? Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?
❒	Sind die bestehende Richtlinien und Zuständigkeiten allen Zielpersonen bekannt?
❒	Gibt es Checklisten, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Unterweisung etc.)?
❒	Wird die Wirksamkeit von IT-Sicherheitsmaßnahmen regelmäßig überprüft?
❒	Gibt es ein dokumentiertes IT-Sicherheitskonzept?

Sicherheit von IT-Systemen	
❒	Werden vorhandene Schutzmechanismen in Anwendungen und Programmen genutzt?
❒	Werden flächendeckend Viren-Schutzprogramme eingesetzt?
❒	Sind allen Systembenutzern Rollen und Profile zugeordnet worden?
❒	Ist geregelt, auf welche Datenbestände jeder Mitarbeiter zugreifen darf? Gibt es sinnvolle Beschränkungen?
❒	Gibt es verschiedene Rollen und Profile für Administratoren, oder darf jeder Administrator alles?
❒	Ist bekannt und geregelt, welche Privilegien und Rechte Programme haben?
❒	Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst oder wird der Auslieferungszustand beibehalten?
❒	Werden nicht benötigte sicherheitsrelevante Programme und Funktionen konsequent deinstalliert bzw. deaktiviert?
❒	Werden Handbücher und Produktdokumentationen frühzeitig gelesen?
❒	Werden ausführliche Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?

Vernetzung und Internet-Anbindung	
❒	Gibt es eine Firewall?
❒	Werden Konfiguration und Funktionsfähigkeit der Firewall regelmäßig kritisch überprüft und kontrolliert?
❒	Gibt es ein Konzept, welche Daten nach außen angeboten werden müssen?
❒	Ist festgelegt, wie mit gefährlichen Zusatzprogrammen (Plugins) und aktiven Inhalten umgegangen wird?
❒	Sind alle unnötigen Dienste und Programmfunktionen deaktiviert?
❒	Sind Web-Browser und E-Mail-Programm sicher konfiguriert?
❒	Sind die Mitarbeiter ausreichend geschult?

Beachtung von Sicherheitserfordernissen	
❒	Werden vertrauliche Informationen und Datenträger sorgfältig aufbewahrt?
❒	Werden vertrauliche Informationen vor Wartungs- oder Reparaturarbeiten von Datenträgern oder IT-Systemen gelöscht?
❒	Werden Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult?
❒	Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?
❒	Werden bestehende Sicherheitsvorgaben kontrolliert und Verstöße geahndet?

Wartung von IT-Systemen: Umgang mit Updates	
❒	Werden Sicherheits-Updates regelmäßig eingespielt?
❒	Gibt es einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheits-Updates informiert?
❒	Gibt es ein Testkonzept für Softwareänderungen?

Passwörter und Verschlüsselung	
❒	Bieten Programme und Anwendungen Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung? Sind die Sicherheitsmechanismen aktiviert?
❒	Wurden voreingestellte oder leere Passwörter geändert?
❒	Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?
❒	Werden Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert?
❒	Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

Notfallvorsorge	
❒	Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?
❒	Werden alle notwendigen Notfallsituationen behandelt?
❒	Kennt jeder Mitarbeiter den Notfallplan und ist dieser gut zugänglich?

Datensicherung	
❒	Gibt es eine Backupstrategie?
❒	Ist festgelegt, welche Daten wie lange gesichert werden?
❒	Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?
❒	Werden die Sicherungsbänder regelmäßig kontrolliert?
❒	Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?

Infrastruktursicherheit	
❒	Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?
❒	Ist der Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden?
❒	Besteht ein ausreichender Schutz vor Einbrechern?
❒	Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?

Präsidium:

Das Präsidium der Georg-August-Universität Göttingen hat gemeinsam mit dem Vorstand der Universitätsmedizin Göttingen die nachfolgende Organisationsrichtlinie zur IT-Sicherheit der Georg-August-Universität Göttingen und der Universitätsmedizin Göttingen beschlossen (§ 37 Abs. 1 Satz 3 1. Halbsatz NHG in der Fassung der Bekanntmachung vom 26.02.2007 (Nds. GVBl. S. 69); § 63 e Abs. 1 Satz 1 NHG).

Organisationsrichtlinie zur IT-Sicherheit der Georg-August-Universität Göttingen und der Universitätsmedizin Göttingen

Präambel

Der Hochschulbetrieb erfordert in zunehmendem Maß die Integration von Verfahren und Abläufen, die sich auf die Möglichkeiten der Kommunikations- und Informationstechnik (IT) stützen. Funktionierende und sichere IT-Prozesse sind daher eine zentrale Grundlage für die Leistungsfähigkeit der Universität und ihrer Verwaltung auf den Gebieten der Forschung, Lehre, Krankenversorgung, der Dienstleistungen im öffentlichen Gesundheitswesen, der Aus-, Fort- und Weiterbildung sowie des Technologietransfers.

Unter diesen Bedingungen kommt der „Sicherheit in der Informationstechnik“ (IT-Sicherheit) eine grundsätzliche und strategische Bedeutung zu, die die Entwicklung und Umsetzung einer einheitlichen hochschulweiten Rahmenrichtlinie der IT-Sicherheit für die Hochschule erforderlich macht. Nicht zuletzt sind sichere IT-Prozesse eine Grundvoraussetzung für alle Datenschutzmaßnahmen, die vor allem bei der Verarbeitung personenbezogener Daten umzusetzen sind.

Dieses kann wegen der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten und der begrenzten finanziellen und personellen Möglichkeiten nur in einem kontinuierlichen IT-Sicherheitsprozess erfolgen. Die Entwicklung und Fortschreibung dieses IT-Sicherheitsprozesses muss sich einerseits an den Aufgaben und Rechten der Hochschule orientieren, andererseits ist sie nur über einen kontinuierlichen IT-Sicherheitsprozesses innerhalb geregelter Verantwortungsstrukturen zu erzielen.

Ziel der Organisationsrichtlinie zur IT-Sicherheit ist es nicht nur, die existierenden rechtlichen Auflagen zu erfüllen, sondern primär die in der Hochschule verarbeiteten, übertragenen und gespeicherten Daten und Anwendungen zu schützen sowie die Hochschule - soweit möglich - vor materiellen und immateriellen Schäden zu bewahren.

Ausdrücklich wird darauf hingewiesen, dass die erfolgreiche Umsetzung des IT-Sicherheitsprozesses die Unterstützung aller Mitarbeiterinnen und Mitarbeiter[1] sowie aller Angehörigen der Universität und der Universitätsmedizin voraussetzt.

1 Gegenstand der Richtlinie

Die Richtlinie legt die Zuständigkeiten, die Verantwortungsstrukturen, die Aufgabenzuordnung und die Zusammenarbeit der Beteiligten im hochschulweiten IT-Sicherheitsprozess sowie dessen Finanzierung fest.

2 Geltungsbereich

Diese Richtlinie gilt für alle Einrichtungen der Universität und der Universitätsmedizin, für deren gesamte IT-Infrastruktur einschließlich der betriebenen IT-Systeme sowie die Gesamtheit der Benutzer.

3 IT-Sicherheitskonzept

(1) Das IT-Sicherheitskonzept der Universität basiert auf

- dieser Richtlinie zur IT-Sicherheit,
- der in den Amtlichen Mitteilungen veröffentlichten IT-Sicherheitsrahmenrichtlinie der Universität einschließlich der Universitätsmedizin,
- der Nutzungsregelung für die IT-Infrastruktur der Universitätsmedizin und
- Einzelregelungen, auf die in der IT-Sicherheitsrahmenrichtlinie verwiesen wird.

(2) Das Sicherheitskonzept orientiert sich am Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI).

4 Organisationsstruktur des IT-Sicherheitsprozesses

(1) Die Verantwortung für die IT-Sicherheit und den IT-Sicherheitsprozess liegt beim Präsidium für die Universität und beim Vorstand für die Universitätsmedizin.

(2) Die Koordinierung des IT-Sicherheitsprozesses obliegt der Arbeitsgruppe „IT-Strategie“ des Präsidiums der Universität und des Vorstands der Universitätsmedizin in ihrer Funktion als Chief Information Office (CIO) der Universität und der Universitätsmedizin.

[1] 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.

In der Arbeitsgruppe „IT-Strategie“ sind vertreten:

- das Präsidiumsmitglied für IT,
- das Präsidiumsmitglied für Bibliothekswesen,
- das Mitglied des Vorstands für Wirtschaftsführung und Administration und
- weitere vom Präsidium und Vorstand benannte Mitglieder.

(3) Die Arbeitsgruppe „IT-Strategie“ setzt die Arbeitsgruppe „IT-Sicherheit“ ein.
Die Arbeitsgruppe „IT-Sicherheit“ wird gebildet aus

- je einem Vertreter der Rechenzentren (GWDG und G3-7) sowie einem Vertreter der NSUB Göttingen,
- den Datenschutzbeauftragten der Universität und der Universitätsmedizin und
- weiteren von der Arbeitsgruppe „IT-Strategie“ benannten Mitgliedern.

(4) Die Leiter der Einrichtungen sind für die Umsetzung von IT-Sicherheit in ihren Einrichtungen verantwortlich. Den Leitern der Einrichtungen wird empfohlen, der Arbeitsgruppe „IT-Sicherheit“
IT-Beauftragte für ihre Einrichtungen zu benennen und diese mit der Umsetzung des IT-Sicherheitsprozesses innerhalb der Einrichtung zu beauftragen. Werden keine IT-Beauftragten benannt, so ist die Funktion des IT-Beauftragten vom Leiter der Einrichtung wahrzunehmen.
(5) Mehrere Einrichtungen können einen gemeinsamen IT-Beauftragten benennen. Die Funktion des IT-Beauftragten kann dabei auch auf der übergeordneten Organisationsebene angesiedelt werden.

5 Aufgaben der Beteiligten

(1) Die Arbeitsgruppe „IT-Strategie“ koordiniert den IT-Sicherheitsprozess.
(2) Die Arbeitsgruppen „IT-Strategie“ und „IT-Sicherheit“ beraten das Präsidium der Universität und den Vorstand der Universitätsmedizin in Fragen der IT-Sicherheit.
(3) Die Arbeitsgruppe „IT-Sicherheit“ erarbeitet und überarbeitet Vorlagen für die hochschulinternen technischen Standards, Richtlinien und Notfallpläne zur IT-Sicherheit, die durch das Präsidium der Universität und den Vorstand der Universitätsmedizin in Kraft gesetzt werden, und unterstützt die Arbeitsgruppe „IT-Strategie“ bei der Umsetzung und Überwachung des IT-Sicherheitsprozesses. Die Arbeitsgruppe „IT-Sicherheit“ koordiniert die Schulung und Weiterbildung der IT-Beauftragten und unterstützt diese bei der Richtlinienumsetzung. Die Arbeitsgruppe „IT-Sicherheit“ erstellt in Abstimmung mit der Arbeitsgruppe „IT-Strategie“ jährlich einen IT-Sicherheitsbericht für das Präsidium der Universität und den Vorstand der Universitätsmedizin.
(4) Die IT-Beauftragten überwachen kontinuierlich die Umsetzung des IT-Sicherheitsprozesses in ihren jeweiligen Verantwortungsbereichen. Dafür müssen sie von der Leitung der jeweiligen Einrichtung mit entsprechenden Kompetenzen ausgestattet werden. Sie informieren regelmäßig sowohl die Leitung ihrer Einrichtung als

auch die Arbeitsgruppe „IT-Sicherheit“ über den Stand der Umsetzung. Sie melden sicherheitsrelevante Vorfälle unverzüglich der Arbeitsgruppe „IT-Sicherheit“ und der Leitung der Einrichtung. Sie sind verpflichtet sich auf dem Gebiet der IT-Sicherheit weiterzubilden und ihr Wissen auf dem aktuellen Stand zu halten. Sie werden hierbei von der Leitung der jeweiligen Einrichtung unterstützt.

(5) Alle Angehörigen und Mitarbeiter der Hochschule sind verpflichtet, sicherheitsrelevante Vorfälle unverzüglich dem zuständigen IT-Beauftragten zu melden.

(6) Die Rechenzentren sind für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit verantwortlich. Sie arbeiten eng mit den Arbeitsgruppen „IT-Strategie“ und „IT-Sicherheit“ zusammen.

6 Gefahrenintervention

(1) Um eine Gefahr für die IT-Sicherheit abzuwehren, treffen die Rechenzentren (GWDG bzw. G3-7) die erforderlichen Maßnahmen; diese können auch die Sperrung von Netzanschlüssen und Benutzerkonten (auch ohne vorherige Benachrichtigung der Betroffenen) beinhalten. Der zuständige IT-Beauftragte sowie die Arbeitsgruppe „IT-Sicherheit“ sind unverzüglich zu informieren. Die Aufhebung der Gefahrenabwehrmaßnahmen durch die Rechenzentren erfolgt nach der Durchführung hinreichender IT-Sicherheitsmaßnahmen in Abstimmung mit der Arbeitsgruppe „IT-Sicherheit“; der zuständige IT-Beauftragte ist zu informieren.

(2) Wenn es zur Abwehr einer akuten Gefahr für die IT-Sicherheit erforderlich ist, treffen die IT-Beauftragten die erforderlichen Maßnahmen; dies kann auch die Stilllegung von IT-Systemen in ihrem Verantwortungsbereich bedeuten. Die Arbeitsgruppe „IT-Sicherheit“ und die Leitung der Einrichtung sind unverzüglich zu informieren. Die Aufhebung der Gefahrenabwehrmaßnahmen durch die IT-Beauftragten erfolgt nach Durchführung hinreichender IT-Sicherheitsmaßnahmen in Abstimmung mit der Arbeitsgruppe „IT-Sicherheit“.

7 Finanzierung

Die personellen und finanziellen Ressourcen aller zentralen und dezentralen IT-Sicherheitsmaßnahmen sind aus den Budgetmitteln der IT-Dienstleister, Zentralverwaltung, zentralen Einrichtungen und Fakultäten zu finanzieren. Hierunter fallen auch zentral und dezentral angebotene Schulungsmaßnahmen für IT-Beauftragte und Benutzer.

8 Inkrafttreten

Diese Richtlinie wird vom Präsidium der Universität und vom Vorstand der Universitätsmedizin verabschiedet. Sie tritt am Tag nach ihrer Bekanntmachung in den Amtlichen Mitteilungen der Universität in Kraft.

Göttingen, 31. JAN. 2007

Für die Georg-August-Universität Göttingen
(ohne Universitätsmedizin)
- Der Präsident -

Prof. Dr. Kurt von Figura

Göttingen, 27. MRZ. 2007

Für die Universitätsmedizin Göttingen
- Der Sprecher des Vorstands -

Prof. Dr. Cornelius Frömmel