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] 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.

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.
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, 31.01.2007

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

gez.
Prof. Dr. Kurt von Figura

Göttingen, 27.03.2007

Für die Universitätsmedizin Göttingen
- Der Sprecher des Vorstands -

gez.
Prof. Dr. Cornelius Frömmel