GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Datum: 24.01.2020 Nr.: 4

Amtliche Mitteilungen I

Inhaltsverzeichnis

Herausgegeben von dem Präsidenten der Georg-August-Universität Göttingen

Redaktion:
Abteilung Wissenschaftsrecht
und Trägerstiftung

Von-Siebold-Str. 2
37075 Göttingen

Telefon:
+49 551/39-24496

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

Präsidium und Vorstand der Universitätsmedizin:

Das Präsidium der Georg-August-Universität Göttingen und der Vorstand der Universitätsmedizin Göttingen haben jeweils am 01.10.2019 nach Empfehlung der Senatskommission für Informationsmanagement (KIM) am 09.05.2019 und nach Stellungnahme des Senats und des Fakultätsrats der Medizinischen Fakultät am 22.05.2019 und am 27.05.2019 die Neufassung der Richtlinie zur Informationssicherheit der Georg-August-Universität Göttingen/ Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts beschlossen (§ 37 Abs. 1 Satz 3 1. Halbsatz NHG; § 63 e Abs. 1 Satz 1 NHG; § 41 Abs. 2 Satz 2 NHG; § 63 h Abs. 2 Satz 2 NHG).

Die Mitbestimmung des Personalrats der Universität und des Personalrats der Universitätsmedizin Göttingen sind am 18.12.2019 und am 17.12.2019 erfolgt (§ 66 Abs. 1 Nr. 10. NPersVG).

Richtlinie
zur Informationssicherheit der Georg-August-Universität Göttingen/ Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts
– Informationssicherheitsrichtlinie (ISRL) –

Inhaltsverzeichnis

Abschnitt I: Grundsätze

§ 1 Gegenstand und Geltungsbereich

(1) Die Informationssicherheitsrichtlinie legt die Verantwortungsstrukturen, die Aufgabenzuordnung und die Zusammenarbeit der Beteiligten sowie inhaltliche Festlegungen im hochschulweiten Informationssicherheitsprozess fest.

(2) Die Informationssicherheitsrichtlinie gilt für alle Mitglieder und Angehörige der Georg-August-Universität Göttingen/Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts einschließlich Universitätsmedizin Göttingen (nachfolgend insgesamt: Stiftungsuniversität Göttingen), insbesondere wenn sie die IT-Infrastruktur der Stiftungsuniversität Göttingen nutzen oder Daten der Stiftungsuniversität Göttingen verarbeiten, und für die gesamte IT-Infrastruktur der Stiftungsuniversität Göttingen einschließlich der betriebenen IT-Systeme.

§ 2 Rahmenbedingungen

(1) Der Betrieb einer Universität und eines Klinikums der Maximalversorgung 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 insbesondere auf den Gebieten der Forschung, Lehre, Krankenversorgung, der Dienstleistungen im öffentlichen Gesundheitswesen, der Aus-, Fort- und Weiterbildung sowie des Technologietransfers.

(2) Hierbei kommt der Informationssicherheit eine grundsätzliche und strategische Bedeutung zu, welche die Entwicklung und Umsetzung einer einheitlichen hochschulweiten Informationssicherheitsrichtlinie für die Universität erforderlich macht. Nicht zuletzt sind sichere IT-Prozesse eine Grundvoraussetzung für alle Datenschutzmaßnahmen, die bei der Verarbeitung personenbezogener Daten umzusetzen sind.

(3) Dieses kann wegen der komplexen Materie, der sich schnell weiter entwickelnden technischen Möglichkeiten und der begrenzten finanziellen und personellen Möglichkeiten nur in einem kontinuierlichen Informationssicherheitsprozess erfolgen. Die Entwicklung und Fortschreibung dieses Informationssicherheitsprozesses müssen sich einerseits an den Aufgaben und Rechten der Universität orientieren, andererseits sind sie nur über einen kontinuierlichen Informationssicherheitsprozess innerhalb geregelter Verantwortungsstrukturen möglich.

(4) Ziel der Informationssicherheitsrichtlinie ist es nicht nur, die existierenden rechtlichen Auflagen zu erfüllen, sondern grundsätzlich die in der Universität verarbeiteten Daten und Anwendungen zu schützen sowie die Universität vor materiellen und immateriellen Schäden zu bewahren, dabei aber auch die Freiheit von Forschung und Lehre, die weltweite Zusammenarbeit auf Basis fachlichen Austauschs, die häufige Projektförmigkeit, die hohe Personalfluktuation, die verschiedenen Mitgliedergruppen mit ihren unterschiedlichen Rollen und Rechten und die schnellen Entwicklungszyklen der Informationstechnik zu berücksichtigen.

§ 3 Sicherheitsziele

(1) Im Sinne dieser Richtlinie ist Informationssicherheit die Herstellung und Aufrechterhaltung der
   (a) „Vertraulichkeit“; das bedeutet, die Gewährleistung des Zugangs zu und Zugriffs auf Informationen nur für Berechtigte,
   (b) „Integrität“; das bedeutet, die Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden,
   (c) „Verfügbarkeit“; das bedeutet, die Gewährleistung des bedarfsorientierten Zugriffs auf Informationen für Berechtigte.

(2) Durch diese Informationssicherheitsrichtlinie soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um das Eintreten von Informationssicherheitsvorfällen weitestgehend zu minimieren. Die Maßnahmen dienen insbesondere
   (a) der zuverlässigen Unterstützung der Prozesse durch die IT und der Sicherstellung der Kontinuität der Arbeitsabläufe,
   (b) der Patientensicherheit und Behandlungseffektivität in der medizinischen Versorgung durch die Universitätsmedizin Göttingen,
   (c) der Wahrung von Dienst-, Betriebs-, Geschäfts- und sonstigen Geheimnissen,
   (d) der Gewährleistung der aus rechtlichen Vorgaben resultierenden Anforderungen,
   (e) der Gewährleistung des informationellen Selbstbestimmungsrechts der oder des Betroffenen bei der Verarbeitung derer oder dessen personenbezogener Daten,
   (f) der Einhaltung der Ordnung der Georg-August-Universität Göttingen zur Sicherung guter wissenschaftlicher Praxis,
   (g) der Reduzierung der bei einem Informationssicherheitsvorfall entstehenden materiellen und immateriellen Schäden sowie
   (h) der Realisierung sicherer und vertrauenswürdiger Verfahren zur Information, Kommunikation und Transaktion mit außeruniversitären Einrichtungen.

§ 4 Informationssicherheitsprozess

(1) Der Informationssicherheitsprozess dient der Sicherheit der Daten, wobei die Sicherheit der datenverarbeitenden Systeme und Stellen gewährleistet werden muss, und umfasst insbesondere folgende Aufgaben:
   (a) Verantwortlichkeiten zu definieren und festzulegen,
   (b) den Schutzbedarf festzustellen und die Risiken zu erfassen,
   (c) den Zugang zu und den Zugriff auf Informationen sowie Art und Umfang der Autorisierung zu definieren und festzulegen,
   (d) Sicherheits- und Kontrollmaßnahmen entsprechend der Informationssicherheitsrichtlinie festzulegen,
   (e) Sicherheits- und Kontrollmaßnahmen zum Schutz der Informationen umzusetzen,

   zu überprüfen und zu aktualisieren.

(2) Alle Informationen sind Kategorien annähernd gleichen Schutzbedarfs zuzuordnen; dabei bedeutet:

(a) „normaler Schutzbedarf“, dass die Auswirkungen eines Schadens begrenzt und überschaubar wären,

(b) „hoher Schutzbedarf“, dass die Auswirkungen eines Schadens beträchtlich sein könnten,

(c) „sehr hoher Schutzbedarf“, dass die Auswirkungen eines Schadens ein existentiell bedrohliches, katastrophales Ausmaß erreichen könnten.

(3) Auf der Basis möglicher Schadensereignisse und deren Ursachen und Auswirkungen sind unter Berücksichtigung des finanziellen und organisatorischen Aufwands Risiken zu bewerten und in einem Risikobehandlungsplan durch Maßnahmen der Risikominderung, Risikovermeidung, Risikoübertragung oder Risikoakzeptanz zu behandeln. Verbleibende Risiken im Rahmen der Risikoakzeptanz sind zu beschreiben und durch die zuständige Leitung zu verantworten.

Abschnitt II: Organisatorische Festlegungen

§ 5 Präsidium und Vorstand

(1) Die Gesamtverantwortung für die Informationssicherheit und den Informationssicherheitsprozess liegt beim Präsidium für die Universität beziehungsweise beim Vorstand für die Universitätsmedizin Göttingen (UMG).

(2) Das Präsidium und der Vorstand delegieren die Organisation und Durchführung des Informationssicherheitsmanagements in dem in § 11 und § 12 festgelegten Umfang auf die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten (ISB) beziehungsweise auf die Informationssicherheitsmanagerinnen oder Informationssicherheitsmanager (ISM).

(3) Der in Anlage 1 festgelegten zuständigen Leitung der jeweiligen Einheit (nachfolgend: Zuständige Leitung) obliegt auf dezentraler Ebene die Wahrnehmung der in § 8 festgelegten Aufgaben. Das Präsidium beziehungsweise der Vorstand kann die Delegation nach Satz 1 aufheben und selbst entscheiden.

§ 6 IT-Steuerungsgruppe und CIO

(1) Die IT-Steuerungsgruppe und der gemeinsame Chief Information Officer der Universität und der UMG (CIO) nehmen Aufgaben für die IT und somit auch für die Informationssicherheit der Stiftungsuniversität Göttingen wahr.

(2) Die konkreten Verantwortlichkeiten ergeben sich aus der „Geschäftsordnung zur gemeinsamen IT-Governance der Georg-August-Universität und Universitätsmedizin Göttingen für die IT-Steuerungsgruppe und den Chief Information Officer“ in der jeweils geltenden Fassung.

§ 7 IT-Dienstleister

(1) IT-Systeme und IT-Dienstleistungen für die Stiftungsuniversität Göttingen werden primär insbesondere durch folgende IT-Dienstleister kooperativ bereitgestellt:

(a) Abteilung Digitale Bibliothek der Niedersächsischen Staats- und Universitätsbibliothek (SUB),

(b) Abteilung IT der Universität,

(c) Geschäftsbereich Informationstechnologie der UMG,

(d) die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG).

(2) Durch Bereitstellungen professioneller und sicherer IT-Dienstleistungen tragen die IT-Dienstleister wesentlich zur Informationssicherheit der Stiftungsuniversität Göttingen bei.

(3) Wird eine Aufgabe nicht durch die in Absatz (1) genannten IT-Dienstleistern wahrgenommen, können Einrichtungen eigene IT-Systeme und IT-Dienstleistungen nutzen und durch andere Dienstleister betreiben lassen. Die IT-Dienstleister unterstützen bei solchen IT-Systemen in grundlegenden Fragen zum IT-Betrieb und zur Informationssicherheit.

§ 8 Zuständige Leitung

(1) Die zuständige Leitung gemäß Anlage 1 kann im jeweiligen Verantwortungsbereich nachgeordnete Leitungen einer Untergliederung mit der Wahrnehmung ihrer Aufgaben beauftragen, die damit zur zuständigen Leitung in ihrem Verantwortungsbereich werden. Dies ist zu dokumentieren und der oder dem ISM mitzuteilen. Die vertretungsweise Wahrnehmung dieser Aufgaben durch eine Abwesenheitsvertretung bleibt unberührt.

(2) Die zuständige Leitung ist in ihrem Verantwortungsbereich verantwortlich für:

a) die Benennung einer Informationssicherheitskoordinatorin oder eines Informationssicherheitskoordinators nach Absatz (3),

b) die Benennung von Fachverantwortlichen nach Absatz (5),

c) die Beschlussfassung über die jeweiligen spezifischen Informationssicherheitskonzepte nach Absatz (6)

d) Entscheidung über die weitere Behandlung von Informationssicherheitsvorfällen nach § 16.

(3) Die zuständige Leitung kann für die jeweilige Einheit eine Beschäftigte oder einen Beschäftigten der Stiftungsuniversität Göttingen als Informationssicherheitskoordinatorin oder Informationssicherheitskoordinator (ISK) benennen. Die Benennung ist zu dokumentieren. Wird keine oder kein ISK benannt, obliegen deren oder dessen Aufgaben der zuständigen Leitung. Die zuständige Leitung kann für die oder den ISK auch eine oder mehrere Stellvertretungen benennen.

(4) Die zuständigen Leitungen können einvernehmlich für ihre Einheiten gemeinsame ISK benennen.

(5) Für die einer Einheit zugeordneten Datenbeständen, IT-Verfahren, IT-Systeme und Infrastrukturen kann die zuständige Leitung eine angemessene Zahl an Fachverantwortliche benennen. Die Benennung ist zu dokumentieren. Soweit keine Fachverantwortliche oder kein Fachverantwortlicher benannt wird, obliegen die Aufgaben der oder des Fachverantwortlichen der zuständigen Leitung.

(6) Die zuständige Leitung beschließt nach Stellungnahme des ISK und Zustimmung des ISB die spezifischen Informationssicherheitskonzepte und verantwortet die in diesen Konzepten übernommen Risiken.

§ 9 Informationssicherheitskoordinatorinnen und Informationssicherheitskoordinatoren (ISK)

(1) Die Informationssicherheitskoordinatorinnen und Informationssicherheitskoordinatoren (ISK) koordinieren innerhalb ihres Verantwortungsbereichs den Informationssicherheitsprozess und überwachen dessen Umsetzung durch die IT-Anwender. Die ISK berichten hierüber der jeweils zuständigen Leitung.

(2) Die zuständige Leitung ist dafür verantwortlich, dass die ISK mit den für die Erfüllung ihrer Aufgaben erforderlichen Befugnissen und Ressourcen ausgestattet sind. Die zuständige Leitung ist verpflichtet, sicherzustellen, dass jene an den erforderlichen Weiterbildungen auf dem Gebiet der Informationssicherheit teilnehmen; die Teilnahme an der Weiterbildung ist eine Pflicht aus dem individuellen Arbeits- bzw. Dienstverhältnis.

(3) Den ISK obliegen insbesondere die folgenden Aufgaben:
   (a) Empfehlung von Sensibilisierungs- und Schulungsmaßnahmen,
   (b) Beratung der Fachverantwortlichen bei der Wahrnehmung ihrer Aufgaben,
   (c) Veranlassung der Erstellung und Aktualisierung von Schutzbedarfsfeststellungen und Risikoanalysen,
   (d) Stellungnahme zu den spezifischen Informationssicherheitskonzepten,
   (e) unverzügliche Vorlage der spezifischen Informationssicherheitskonzepte gegenüber der oder dem ISB,
   (f) Sammlung und Zurverfügungstellung der spezifischen Informationssicherheitskonzepte der jeweiligen Einheit,
   (g) Bewertung der Schwere gemeldeter Informationssicherheitsvorfälle; Prüfung, ob eine Informationssicherheitsvorfall gleichzeitig auch eine Datenschutzvorfall sein könnte und Erstellung einer Handlungsempfehlung gemäß § 16 für die zuständige Leitung,

(4) ISK können zur Aufgabenwahrnehmung die Beratung der oder des ISB und der oder des ISM in Anspruch nehmen.

§ 10 Fachverantwortliche

(1) Fachverantwortliche sind bzgl. der ihnen zugeordneten Datenbeständen, IT-Verfahren, IT-Systeme und Infrastrukturen für die Umsetzung des Informationssicherheitsprozesses verantwortlich, was insbesondere die folgenden Aufgaben umfasst:
   (a) Feststellung des Schutzbedarfs von Informationen, IT-Verfahren, IT-Systemen und Infrastrukturen sowie Analysierung der Risiken,
   (b) Erstellung und Fortschreibung der spezifischen Informationssicherheitskonzepte auf Basis von Schutzbedarfsfeststellung und Risikoanalyse,
   (c) regelmäßige Überprüfung der Schutzbedarfsfeststellung, Risikoanalyse und des spezifischen Informationssicherheitskonzepts entsprechend der im spezifischen Informationssicherheitskonzept festzulegenden Intervallen,
   (d) Veranlassung und Kontrolle der Umsetzung der Maßnahmen des spezifischen Informationssicherheitskonzepts, insbesondere auch bei Inanspruchnahme externer IT-Dienstleister (z.B. Auftragsverarbeitung).

(2) Fachverantwortliche können zur Wahrnehmung ihrer Aufgaben die Beratung der oder des ISK, der oder des ISB, des IT-Personals der jeweiligen Einheit oder der internen IT-Dienstleister anfordern.

(3) Ergebnis einer Schutzbedarfsfeststellung und Risikoanalyse kann auch sein, dass für einen Datenbestand, ein IT-Verfahren, ein IT-System oder eine Infrastruktur über die Umsetzung der Informationssicherheitsrichtlinie und des Maßnahmenkatalogs für den IT-Grundschutz (Anlage 2) hinaus keine weiteren Maßnahmen erforderlich sind.

§ 11 Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter (ISB)

(1) Präsidium und Vorstand benennen eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten (ISB). Die Benennung ist zu dokumentieren.

(2) Die oder der ISB hat insbesondere die folgenden Aufgaben:
   (a) Koordinierung und Weiterentwicklung des Informationssicherheitsprozesses für die Stiftungsuniversität Göttingen,
   (b) Entwicklung von Empfehlungen für Präsidium und Vorstand für folgende Themenfelder:
      (i) Erstellung und Fortschreibung des Maßnahmenkatalogs für den IT-Grundschutz,
      (ii) ergänzende Informationen zur Informationssicherheitsrichtlinie (z. B. Empfehlungen für hochschulinterne technische Standards, Musterlösungen, und Notfallpläne),
      (iii) Änderungen zu spezifischen Informationssicherheitskonzepten auf Grund von Sicherheitsvorfällen (im Sinne von § 16 Abs. (5)),
      (iv) Schulungskonzepte.
   (c) Beratung folgender Stellen:
      (i) Präsidium, Vorstand, IT-Steuerungsgruppe und CIO in Fragen der Informationssicherheit,
      (ii) Leitungen der IT-Dienstleister,
      (iii) Datenschutzbeauftragte und Datenschutzmanagerinnen oder Datenschutzmanager bezüglich technischer und organisatorischer Maßnahmen,
      (iv) Einheiten bei der Umsetzung der Informationssicherheitsrichtlinie,
      (v) ISK bei der Beseitigung von Gefahren für die Informationssicherheit,
      (vi) Fachverantwortliche bei der Erstellung von spezifischen Informationssicherheitskonzepten.
   (d) Zustimmung zu den spezifischen Informationssicherheitskonzepten der Einheiten; im Dissensfall entscheidet das Präsidium beziehungsweise der Vorstand,
   (e) Erstellung und Aktualisierung eines Verzeichnisses aller spezifischen Informationssicherheitskonzepte,
   (f) Bewertung von Informationssicherheitsvorfällen und Ableitung von strukturellen und konzeptionellen Empfehlungen gemäß § 16,
   (g) Erstellung des jährlichen Berichts für Präsidium und Vorstand zur Informationssicherheit einschließlich Empfehlungen zur Überarbeitung dieser Informationssicherheitsrichtlinie und anderer übergreifender Informationssicherheitskonzepte; bei Bedarf erfolgt die Berichterstattung auch darüber hinaus.

(3) Die oder der ISB hat im Informationssicherheitsprozess Fragen betreffend den Datenschutz zu berücksichtigen und bei Zielkonflikten zwischen Informationssicherheit und Datenschutz zu Konzepten und Maßnahmen den Datenschutzbeauftragten einzubinden.

§ 12 Informationssicherheitsmanagerinnen oder Informationssicherheitsmanager (ISM)

(1) Präsidium beziehungsweise Vorstand benennen für die Universität beziehungsweise die Universitätsmedizin jeweils eine Informationssicherheitsmanagerin oder einen Informationssicherheitsmanager (ISM).

(2) Die oder der ISM hat insbesondere die folgenden Aufgaben:

(a) Beauftragung mit der Steuerung und Überwachung der Umsetzung von Informationssicherheitsmaßnahmen im Rahmen der Risikobehandlungspläne einschließlich Sensibilisierungs- und Schulungsmaßnahmen sowie Dokumentation der Maßnahmen im jeweiligen Verantwortungsbereich,

(b) Bewertung und Weiterleitung von Meldungen zu Informationssicherheitsvorfällen und Erstellung von Handlungsempfehlungen für die Behandlung der Informationssicherheitsvorfälle im operativen Bereich gemäß § 16 Abs. (4).

(c) Erstellung des Berichts zur Informationssicherheit, soweit es

(i) Fortschritte und Probleme bei der Umsetzung von Informationssicherheitsmaßnahmen (operative Aspekte) oder

(ii) Informationssicherheitsvorfälle

im jeweiligen Verantwortungsbereich betrifft.

§ 13 Datenschutz- und Informationssicherheits-Beirat (DIB)

(1) Das Datenschutz- und Informationssicherheits-Beirat (DIB) besteht aus:

(a) der oder dem ISB,

(b) der Stellvertreterin oder dem Stellvertreter der oder des ISB,

(c) den ISM der Universität und der UMG,

(d) den Datenschutzbeauftragten (DSB) der Universität, der UMG und der GWDG,

(e) den Datenschutzmanagerinnen oder Datenschutzmanagern (DSM) der Universität und der UMG,

(f) je einer Vertreterin oder einem Vertreter der GWDG, des Geschäftsbereichs Informationstechnologie der UMG, der SUB und der Abteilung IT der Universität,

(g) zwei Vertreterinnen oder Vertreter der Fakultäten der Universität und ein Vertreter der Medizinischen Fakultät,

(h) einer Vertreterin oder einem Vertreter des Ressorts 2 Krankenversorgung der UMG,

(i) je einer Vertreterin oder einem Vertreter der Abteilungen und Stabsstellen der Zentralverwaltung und des Ressorts 3 Wirtschaftsführung und Administration der UMG,

(j) je einem Mitglied des Personalrats der Universität und der UMG sowie

(k) weiteren von der oder dem ISB bei Bedarf benannten Personen.

(2) Die Sitzungen des DIB finden statt, sooft es die Geschäftslage erfordert, mindestens aber viermal im Jahr. Die Sitzungen werden von der oder dem ISB einberufen und geleitet.

(3) Das DIB dient den folgenden Zwecken:

(a) Informationsaustausch zwischen den am Informationssicherheitsprozess und am Datenschutzprozess Beteiligten,

(b) Berücksichtigung von Interessen der Bereiche Forschung und Lehre, Krankenversorgung und Verwaltung sowie der Beteiligten im Informationssicherheitsprozess,

(c) Einbindung der IT-Dienstleister in den Informationssicherheitsprozess,

(d) Beratung der oder des ISB, der DSB sowie der oder des ISM und der oder des DSM in Fragen der Informationssicherheit und des Datenschutzes,

(e) Erarbeitung von Empfehlungen zur Änderung der Informationssicherheitsrichtlinie und übergreifender Informationssicherheitskonzepte und zum Datenschutz.

Abschnitt III: Inhaltliche Festlegungen

§ 14 Maßnahmenkatalog für den IT-Grundschutz

(1) Inhaltliche Festlegungen für IT-Systeme mit normalem Schutzbedarf (IT-Grundschutz) werden im „Maßnahmenkatalog für den IT-Grundschutz“ definiert, der sich in Maßnahmen für IT-Anwender und IT-Personal unterteilt.

(2) Die Bestimmungen im Maßnahmenkatalog sind verbindlich; von ihnen kann ausschließlich nach Maßgabe von Absatz (3) abgewichen werden.

(3) Vom Maßnahmenkatalog abweichende Bestimmungen können in spezifischen Informationssicherheitskonzepten für abgegrenzte Datenbestände, Bereiche der IT-Infrastruktur oder IT-Systeme unter Berücksichtigung spezifischer Risiken und Schutzanforderungen erstellt werden, soweit keine Informationssicherheits- oder Datenschutzanforderungen bezüglich der zu verarbeitenden Daten oder der IT-Infrastruktur dem entgegenstehen.

(4) Die GWDG als IT-Dienstleister für die Universität ist vertraglich auf die Informationssicherheitsrichtlinie zu verpflichten.

(5) Externe IT-Dienstleister, die mit der Wahrnehmung von Aufgaben an IT-Systemen beauftragt werden, sind auf die Informationssicherheitsrichtlinie zu verpflichten, soweit dies unter Berücksichtigung des Schutzbedarfs angemessen ist. Die Einhaltung der Informationssicherheitsrichtlinie durch die externen IT-Dienstleister ist durch das zuständige IT-Personal des Auftraggebers zu überprüfen. Externe IT-Dienstleister sind darauf zu verpflichten, die Auftraggeber auf Risiken, die durch die von ihnen erbrachten Dienstleistungen im IT-System entstehen, hinzuweisen.

§ 15 Zusätzliche Maßnahmen

(1) Für alle IT-Systeme ist durch die jeweiligen Fachverantwortlichen zu prüfen, ob ein über den IT-Grundschutz hinausgehender höherer Schutzbedarf besteht.

(2) Wird ein höherer Schutzbedarf festgestellt, so sind zusätzliche Maßnahmen im Rahmen eines spezifischen Informationssicherheitskonzepts von den Fachverantwortlichen festzulegen.

(3) IT-Systeme, für die ein höherer Schutzbedarf festgestellt wurde, dürfen erst in Betrieb genommen werden, nachdem für diese eine auf einer Risikobewertung basierendes spezifisches Informationssicherheitskonzept beschlossen, umgesetzt und der Betrieb freigegeben wurde.

§ 16 Umgang mit Informationssicherheitsvorfällen

(1) Mitglieder und Angehörige der Stiftungsuniversität Göttingen haben für die Informationssicherheit relevante Vorfälle (Informationssicherheitsvorfälle) unverzüglich der oder dem zuständigen ISK mitzuteilen.

(2) Die oder der ISK bewertet die Schwere des Informationssicherheitsvorfalls und leitet ihre oder seine Handlungsempfehlung an die zuständige Leitung weiter.

(3) Die zuständige Leitung entscheidet über die weitere Behandlung des Informationssicherheitsvorfalls. Die Leitung entscheidet dabei auch, ob die oder der ISM auf Grund der Schwere des Informationssicherheitsvorfalls zu informieren ist, und informiert erforderlichenfalls selbst oder durch die oder den ISK unverzüglich die oder

den ISM. Informationssicherheitsvorfälle, die den Datenschutz betreffen, sind der oder dem DSM und der oder dem ISM zu melden.

(4) Die oder der ISM informiert die oder den ISB über den gemeldeten Informationssicherheitsvorfall und holt dessen Stellungnahme ein. Die oder der ISM informiert Präsidium beziehungsweise Vorstand in Abhängigkeit von der eigenen Bewertung und der Stellungnahme der oder das ISB unverzüglich und/oder zusammenfassend im Bericht zur Informationssicherheit über den gemeldeten Informationssicherheitsvorfall. Die oder der ISM erstellt im Benehmen mit der oder dem ISB Handlungsempfehlungen zur operativen Bearbeitung des Informationssicherheitsvorfalls für die zuständige Stelle.

(5) Die oder der ISB prüft nach einem Informationssicherheitsvorfall, ob zu Regelungen zur Informationssicherheit, insbesondere zu Richtlinien, übergreifenden und spezifischen Informationssicherheitskonzepten ein Änderungsbedarf besteht und erstellt nach Stellungnahme von ISM, der oder des zuständigen ISK, der zuständigen Leitung und dem DIB Empfehlungen für Präsidium, Vorstand, zuständige Leitungen und die ISK.

(6) Die oder der ISM meldet Informationssicherheitsvorfälle an die zuständigen Behörden. Soweit Informationssicherheitsvorfälle zugleich Datenschutzvorfälle darstellen, erfolgt die Meldung an die hierfür zuständigen Behörden durch den DSM.

(7) Das Nähere zum Umgang mit Informationssicherheitsvorfällen können das Präsidium beziehungsweise der Vorstand in einer Richtlinie regeln.

§ 17 Gefahrenintervention

(1) Um eine gegenwärtige Gefahr für die Informationssicherheit abzuwehren, treffen IT-Personal und interne IT-Dienstleister (einschließlich der GWDG) in ihrem jeweiligen Verantwortungsbereich die erforderlichen Maßnahmen, um die Einwirkung des schädigenden Ereignisses zu verhindern oder zu beenden; sofern es sich zudem um eine erhebliche Gefahr handelt, können als erforderliche Maßnahmen auch die Sperrung von Netzanschlüssen und Nutzerkonten ergriffen werden.

(2) Bei Vorliegen eines wichtigen Grundes kann die Sperrung auch ohne vorherige Benachrichtigung der von der Sperrung Betroffenen vorgenommen werden.

(3) Die oder der zuständige ISK sowie die oder der ISM sind unverzüglich zu informieren.

(4) Die Aufhebung der Maßnahmen erfolgt nach der Durchführung der erforderlichen IT-Sicherheitsmaßnahmen mit Zustimmung der oder des ISM und der oder des ISK.

Abschnitt IV: Schlussbestimmungen

In- und Außerkrafttreten

(1) Die Richtlinie zur Informationssicherheit der Georg-August-Universität Göttingen/Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Mitteilungen I der Georg-August-Universität Göttingen in Kraft.

(2) Gleichzeitig tritt die Sicherheitsrahmenrichtlinie der Georg-August-Universität Göttingen

und der Universitätsmedizin Göttingen in der Fassung der Bekanntmachung vom 15.06.2007 (AM 11/2007 S. 493) und die Organisationsrichtlinie zu IT-Sicherheit der Georg-August-Universität Göttingen und der Universitätsmedizin Göttingen in der Fassung der Bekanntmachung vom 15.06.2007 (AM 11/2007 S. 522) außer Kraft.

Anlage 1 Festlegung der zuständigen Leitung der jeweiligen Einheit

Einheit	**Zuständige Leitung**
Fakultäten	die jeweilige Dekanin oder der jeweilige Dekan
fakultätsübergreifenden und zentralen wissenschaftlichen Einrichtungen (z. B. Zentren, Lichtenberg-Kolleg)	die jeweilige geschäftsführende Leiterin oder der jeweilige geschäftsführende Leiter
fakultätsübergreifenden und zentralen Infrastruktureinrichtungen (z. B. SUB, Labore)	die jeweilige Leiterin oder der jeweilige Leiter
Einrichtungen für besondere Aufgaben (z. B. XLAB)	die jeweilige geschäftsführende Leiterin oder der jeweilige geschäftsführende Leiter
Abteilungen und Stabsstellen der Zentralverwaltung	die jeweilige Leiterin oder der jeweilige Leiter
Kliniken und Institute der UMG	die jeweilige Leiterin oder der jeweilige Leiter
Referate, Geschäftsbereiche und zentrale Einrichtungen der Krankenversorgung beziehungsweise Administration der UMG	die jeweilige Leiterin oder der jeweilige Leiter

Anlage 2 Maßnahmenkatalog für den IT-Grundschutz

A. Maßnahmen für Anwender

A.1 Anwenderqualifizierung

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	ISK

(1) Die Mitarbeiter sind aufgabenspezifisch für die am Arbeitsplatz eingesetzten IT-Verfahren zu schulen. Schulungsziele sind:

(a) Sicherer Umgang mit der Anwendung,

(b) Sensibilisierung für Fragen der Informationssicherheit,

(c) Förderung der Selbsteinschätzung bei auftretenden Problemen (Wann sollten Experten hinzugezogen werden?),

(d) Kenntnis über bestehende Bestimmungen,

(e) Kenntnis über die Anforderungen des Datenschutzes.

A.2 Meldung von IT-Problemen

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

(1) IT-Probleme aller Art (Systemabstürze, fehlerhaftes Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u.a.) sind vom jeweiligen IT-Anwender dem zuständigen IT-Personal mitzuteilen.

A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	Zuständige Leitung

(1) Verstöße können disziplinar- oder arbeitsrechtlich geahndet werden. Zudem können Verstöße gegen gesetzliche Bestimmungen (z. B. Datenschutzgesetze, ärztliche Schweigepflicht) als Straftat oder Ordnungswidrigkeit verfolgt werden.

(2) Als Verstoß nach Satz 1 gilt insbesondere die schuldhafte Nichtbeachtung der Informationssicherheitsrichtlinie insbesondere, wenn durch diese

(a) die Sicherheit der Mitglieder oder Angehörigen der Stiftungsuniversität Göttingen, Nutzer, Vertragspartner, Berater in erheblichen Umfang beeinträchtigt wird,

(b) die Sicherheit von Daten, Informationen, IT-Systemen oder der Netze gefährdet wird,

(c) der Stiftungsuniversität Göttingen materielle oder immaterielle Schäden zufügt wird,

(d) der unberechtigte Zugriff auf Systeme und Informationen und deren Preisgabe und/oder Änderung ermöglicht wird,

(e) die Nutzung von Informationen der Stiftungsuniversität Göttingen für illegale Zwecke ermöglicht wird und

(f) der unbefugte Zugriff auf personenbezogene Daten und vertrauliche Hochschuldaten ermöglicht wird.

(3) Liegen zureichende tatsächliche Anhaltspunkte für einen Verstoß vor, können durch das IT-Personal, auch ohne Kenntnis der oder des Betroffenen, Maßnahmen durchgeführt werden, die geeignet sind, den durch den Verstoß drohenden Schaden zu verhindern, abzustellen oder zu beweisen. Schon vor Maßnahmenbeginn sind die oder der zuständige Datenschutzbeauftragte und eine Vertretung des jeweiligen Personalrats sowie eine Vertretung der Internen Revision (nachfolgend insgesamt: der zu beteiligenden Stellen) hinzuzuziehen; deren Einverständnis mit den Maßnahmen ist erforderlich für ihre Durchführung. Das die Maßnahmen durchführende IT-Personal informiert über den Verlauf und das Ergebnis der Maßnahmen:

(a) die zu beteiligenden Stellen,

(b) in jedem Fall die Betroffene oder den Betroffenen, gegebenenfalls die vorgesetzte Person und weitere Personen; in allen Fällen in Abstimmung mit den zu beteiligenden Stellen.

(4) Die erhobenen Daten sind unverzüglich nach Abschluss der Maßnahme zu vernichten. Der Abschluss der Maßnahme ist von den zu beteiligenden Stellen festzustellen.

A.4 Kontrollierter Softwareeinsatz

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

(1) Auf IT-Systemen der Stiftungsuniversität Göttingen darf nur Software installiert werden, die zur Erfüllung der dienstlichen und auf das Studium bezogenen Aufgaben erforderlich ist.

(2) Das eigenmächtige Installieren oder Ausführen von zusätzlicher Software ist IT-Anwendern nicht gestattet. Dies betrifft insbesondere auch das Herunterladen von Software aus dem Internet oder das Starten von per E-Mail erhaltener Software.

A.5 Schutz vor Viren und anderer Schadsoftware

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

(1) Auf allen Arbeitsplatzrechnern ist grundsätzlich ein aktueller Virenscanner einzurichten, der automatisch alle Dateien beim Zugriff überprüft. Damit soll bereits das Eindringen von schädlichen Programmen erkannt und verhindert werden.

(2) Bei Verdacht auf Infektion mit Schadsoftware ist das zuständige IT-Personal zu informieren.

A.6 Zutritts-, Zugangs- und Zugriffskontrolle

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

(1) Räume, in denen Arbeitsplatzcomputer stehen, sind grundsätzlich außerhalb der üblichen Arbeitszeiten (insbesondere nachts und am Wochenende) und bei Abwesenheit zu verschließen. Hiervon darf nur abgewichen werden, soweit es die Arbeitsorganisation dringend erfordert und andere Sicherheitsmaßnahmen es ermöglichen.

(2) Bei Räumen mit Publikumsverkehr sind Bildschirmarbeitsplätze so einzurichten, dass schützenswerte Daten nicht von Unbefugten eingesehen werden können.

(3) Beim Ausdruck schützenswerter Daten muss das Entnehmen der Ausdrucke durch Unbefugte verhindert werden (Sicherstellung der Vertraulichkeit).

A.7 Sperren und ausschalten

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

(1) Beim Verlassen des Arbeitsplatzes ist der Arbeitsplatzrechner durch einen Kennwortschutz zu sperren.

(2) Eine Sperrung muss zusätzlich automatisch zeitgesteuert bei Nicht-Nutzung des Rechners erfolgen.

(3) Grundsätzlich sind die Systeme nach Dienstschluss auszuschalten.

(4) Von den Regeln zum Sperren und Ausschalten darf nur abgewichen werden, soweit es die Arbeitsorganisation dringend erfordert (z.B. bei Mess- und Steuerrechnern) und geeignete Sicherheitsmaßnahmen es ermöglichen.

A.8 Sicherung von Notebooks, mobilen Speichermedien, Smartphones

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

(1) Grundsätzlich sind mobile Endgeräte und Speichermedien durch geeignete Sicherheitsmaßnahmen vor Diebstahl zu schützen.

(2) Der unberechtigte Zugriff auf mobile Endgeräte und darauf gespeicherte Daten muss durch geeignete Zugriffsschutzmaßnahmen (z.B. Passwörter, PINs, biometrische Verfahren) verhindert werden.

(3) Die Speicherung von schutzwürdigen Daten auf Notebooks, mobilen Speichermedien (z. B. Smartphones, USB-Sticks etc.) ist nur dann zulässig, wenn eine dienstliche Notwendigkeit besteht und die Daten entsprechend den jeweiligen aktuellen Sicherheitsanforderungen[1] verschlüsselt werden. Weiterhin ist sicherzustellen, dass der unbefugte Zugriff auf die Daten durch Unberechtigte ausgeschlossen ist.

[1] Algorithmus, Schlüssellänge nach Angaben der Bundesnetzagentur

A.9 Personenbezogene Nutzerkonten

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

(1) Alle dienstlich genutzten IT-Systeme (einschließlich Smartphones) sind so einzurichten, dass nur berechtigte Personen die Möglichkeit haben, auf diese zuzugreifen. Infolgedessen ist zunächst eine Anmeldung mit einem geeigneten Authentisierungsverfahren (Passwort, Smartcard, biometrische Verfahren o.ä.) erforderlich.

(2) Die Vergabe von Nutzerkonten für die Arbeit an IT-Systemen muss personenbezogen erfolgen. Die Arbeit unter dem Nutzerkonto einer anderen Person ist unzulässig.

(3) Vertretungen sind nicht durch Weitergabe von Zugangsdaten personenbezogener Nutzerkonten, sondern durch geeignete Rechtevergaben zu organisieren.

(4) Dem IT-Anwender ist untersagt, die für das Authentisierungsverfahren erforderlichen Zugangsdaten weiterzugeben.

(5) Der Verzicht auf personenbezogene Nutzerkonten ist für IT-Systeme zulässig, bei denen bedingt durch die Arbeitsorganisation ein schneller Nutzerwechsel erforderlich ist (z. B. Leitstellen in der UMG, Lesesaaltheken) oder die für allgemeine öffentliche Zugänge bestimmt sind (z.B. Kiosksysteme, Abfragestationen für Bibliothekskataloge).

A.10 Gebrauch von Passwörtern

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

(1) Jeder Nutzer ist für alle Handlungen verantwortlich, die unter Verwendung seines Nutzerkontos vorgenommen werden.

(2) Die für Nutzung von IT-Systemen der Stiftungsuniversität Göttingen verwendeten Passwörter dürfen nicht mit zur Nutzung von anderen, nicht der Stiftungsuniversität Göttingen zugeordneten IT-Systemen verwendeten Passwörtern identisch oder ähnlich sein.

(3) Für den Umgang mit Passwörtern ist zu beachten:

(a) Passwörter sind nicht auf programmierbaren Funktionstasten zu speichern.

(b) Das Abspeichern von Passwörtern für IT-Systeme der Stiftungsuniversität Göttingen in Anwendungen insbesondere Browsern ist grundsätzlich nicht zulässig. Soweit Ausnahmeregelungen eine Abspeicherung zulassen, ist der Zugriff auf den Passwort-Speicher mit einem Master-Kennwort zu sichern.

(c) Soweit Passwörter z.B. wegen ihrer Vielzahl nicht nur gemerkt werden können, sondern notiert werden müssen, sind diese in einem Passwort-Manager mit sicherem Master-Kennwort zu speichern.

(d) Passwörter auf Papier aufzuschreiben ist zu vermeiden. Soweit ein Aufschreiben nicht vermeidbar ist, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.

(e) Ein Passwort ist zu ändern, wenn es unautorisierten Personen bekannt geworden ist.

(f) Die Eingabe eines Passwortes muss unbeobachtet stattfinden.

(4) Sofern ein IT-System bzw. eine Anwendung keine Passwort-Änderung erzwingt oder explizite Regeln hierfür erlassen wurden, sind grundsätzlich folgende Regeln zur Passwort-Änderung zu befolgen:

(a) Das Passwort ist regelmäßig zu ändern. Als Frist für einen Passwortwechsel wird ein Zeitraum zwischen drei Monaten und einem Jahr empfohlen.

(b) Neue Passwörter müssen sich vom alten Passwort, über mehrere Wechselzyklen hinweg, signifikant unterscheiden.

(5) Sofern ein IT-System bzw. eine Anwendung keine Passwortregeln erzwingt oder für bestimmte Passwörter explizit Regeln erlassen wurden, sind grundsätzlich folgende Regeln zur Passwort-Stärke zu befolgen:

(a) Es sind keine gängigen oder leicht zu erratenden Buchstaben- und/oder Ziffernfolgen, wie z. B. Namen, Kfz-Kennzeichen, Geburtsdaten, einzelne Wörter in deutscher oder anderer Sprache oder nur geringfügig variierte Versionen solcher Zeichenfolgen zu verwenden.

(b) Das Passwort muss mindestens 8 Stellen lang sein. Empfohlen werden 10 Stellen.

(c) Jedes Passwort muss mindestens einen Groß- und einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.

(d) Alternativ kann von (c) abgewichen werden, wenn sichergestellt ist, dass ein gewähltes Passwort z.B. durch höhere Länge genauso sicher ist, wie ein nach (b) und (c) gewähltes.

(6) Erhält ein Nutzer beim Anmelden mit seinem Passwort aus ungeklärten Gründen 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).

(7) Vergisst ein Nutzer sein Passwort, hat er ohne wiederholtes Ausprobieren beim zuständigen IT-Personal oder soweit verfügbar über Self-Service-Funktionen das Zurücksetzen zu veranlassen. Diese Festlegung soll verhindern, dass der Vorgang als Eindringversuch protokolliert und behandelt wird.

A.11 Zugriffsrechte

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

(1) Der Nutzer darf nur mit den Zugriffsrechten ausgestattet werden, die für die Erledigung seiner Dienstaufgaben erforderlich sind. Insbesondere sind Arbeiten, für die nicht zwingend erhöhte Privilegien benötigt werden, nicht mit privilegierten Nutzerkonten („Administrator“, „root“ o.a.) vorzunehmen.

(2) Privilegierte Nutzerkonten dürfen nur an IT-Personal vergeben werden bzw. Personen mit privilegierten Nutzerkonten sind als IT-Personal zu betrachten und haben die Maßnahmen für IT-Personal zu beachten und umzusetzen.

(3) Über technische Maßnahmen hinaus sind auch organisatorische Regeln zu beachten (z.B. für Zugriff auf Patientendaten in der Universitätsmedizin).

A.12 Netzzugänge

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

(1) Der Anschluss von IT-Systemen an das Datennetz der Stiftungsuniversität Göttingen hat ausschließlich über die dafür vorgesehene Infrastruktur zu erfolgen. Die eigenmächtige, d.h. ohne vorherige Zustimmung des Netzbetreibers vorgenommene Einrichtung oder Benutzung von zusätzlichen Netzzugängen (Router, Switches, Modems, WLAN-Accesspoints o.ä.) ist unzulässig.

(2) Die „Netzbetriebsordnung der Universitätsmedizin“ und die „Nutzungsordnung der GWDG“ sind bei der Umsetzung zu beachten.

A.13 Telearbeit

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

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

(2) Zur Einrichtung und zum Betrieb von Telearbeitsplätzen sind die bestehenden Dienstvereinbarungen[2] sowie weitere Regelungen zum Datenschutz und zur Datensicherheit zu beachten.

A.14 Sichere Netzwerknutzung - Allgemeine Anforderungen

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

(1) Der Einsatz von verschlüsselten Kommunikationsdiensten ist soweit technisch möglich unverschlüsselten Diensten vorzuziehen.

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

A.15 Sichere Netzwerknutzung - E-Mail

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

(1) Für die dienstliche E-Mail-Kommunikation ist nur die Verwendung dienstlicher E-Mail-Konten zulässig.

(2) Eine automatisierte Weiterleitung dienstlicher E-Mails an externe Provider (Internetanbieter) ist unzulässig.

(3) Für die elektronische Weitergabe von schützenswerten Daten sind die vorhandenen technischen Lösungen zur sicheren und verschlüsselten Übertragung oder Bereitstellung[3] von Daten zu verwenden.

[2] Siehe Anlage „Mitgeltende Dokumente“
[3] Zum Zeitpunkt der Erstellung der Richtlinie z.B. Cryptshare in der UMG.

(4) Wird auf dienstliche E-Mails von außerhalb der Stiftungsuniversität Göttingen zugegriffen, so sind zwingend verschlüsselte Übertragungsprotokolle zu verwenden. Es sind die Regelungen von Maßnahme A.8 zu beachten.

(5) Wird auf dienstliche E-Mails von nicht universitätseigenen IT-Systemen zugegriffen, so ist sicherzustellen, dass auf den fremden Systemen keine Inhalte nach der Nutzung verbleiben.

(6) Es ist grundsätzlich untersagt, sich über in E-Mails hinterlegte Internetlinks anzumelden. Davon ausgenommen sind E-Mails, die zur Identitätsbestätigung bei Anmeldungen an Diensten durch eigene Handlungen ausgelöst wurden.

(7) Es ist ausdrücklich untersagt, in E-Mails enthaltenen Aufforderungen zur Preisgabe von Zugangsdaten zu folgen.

(8) Per E-Mail erhaltene Anhänge und Internetlinks sind nur dann zu öffnen, wenn ihre Ungefährlichkeit, z.B. durch Herkunft und Kontext, anzunehmen ist.

A.16 Datenspeicherung

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

(1) Dienstliche Daten sind grundsätzlich innerhalb der IT-Systeme der Stiftungsuniversität Göttingen (einschließlich der von der GWDG für die Stiftungsuniversität betriebenen IT-Systeme) zu speichern.

(2) Dabei sind die Möglichkeiten der Speicherung auf zentralen Servern zu nutzen.

(3) Das Speichern schützenswerter Daten auf der Festplatte des Arbeitsplatzrechners oder anderer lokaler Speichermedien ist nur zulässig, wenn das spezifische Informationssicherheitskonzept für den jeweiligen Datenbestand dies zulässt und die darin festgelegten Sicherheitsmaßnahmen getroffen wurden.

(4) Die Speicherung (und Verarbeitung) dienstlicher Daten außerhalb der IT-Systeme der Stiftungsuniversität Göttingen (z.B. auf Cloud-Diensten oder privaten Geräten) ist nur zulässig, wenn dies dienstlich erforderlich ist und das spezifische Informationssicherheitskonzept für den jeweiligen Datenbestand diese Speicherung zulässt. Bei einer externen Speicherung ist eine dem Schutzbedarf angemessene Sicherung der Daten gegen Verlust der Daten, der Vertraulichkeit und der Integrität der Daten zu gewährleisten. Möglichkeiten zur Rückholung der Daten vom und deren Löschung auf dem externen Speicher müssen sichergestellt sein.

(5) Die Speicherung schutzwürdiger Daten außerhalb der IT-Systeme der Stiftungsuniversität Göttingen ist nur in den Staaten des europäischen Wirtschaftsraums und sicheren Drittstaaten entsprechend dem Datenschutzrecht zulässig.

A.17 Nutzung externer Dienste

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

(1) Die Nutzung externer Kommunikationsdienste (z.B. Skype, Teamviewer) ermöglicht Zugriffe aus dem Internet auf IT-Systeme der Stiftungsuniversität Göttingen.

(2) Die Nutzung solcher Dienste ist nur zulässig, wenn die spezifischen Informationssicherheitskonzepte für die auf den genutzten Rechner verarbeiteten Daten und die genutzten Teilbereiche der Infrastruktur den Einsatz erlauben.

A.18 Nutzung privater Hard- und Software

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

(1) Die Benutzung von privater Hard- und Software ist in Verbindung mit der IT-Infrastruktur der Stiftungsuniversität Göttingen nur erlaubt, wenn die spezifischen Informationssicherheitskonzepte für den jeweiligen Teilbereich der Infrastruktur dies erlauben.

(2) Ausdrücklich erlaubt ist der Einsatz von privaten Geräten in speziell vorgesehenen Bereichen und dafür vorgesehen Anschlüssen in Bibliotheken, an Anschlüssen für Dozenten in Hörsälen und Seminarräumen, in Studierendenarbeitsbereichen und allgemein in den Funknetzen eduroam und GuestOnCampus der Stiftungsuniversität Göttingen.

(3) Die Zulassung von privaten Geräten in anderen Teilen der Infrastruktur der Stiftungsuniversität Göttingen setzt zwingend voraus, dass dort angeschlossene Endgeräte den Anforderungen der Maßnahmenkataloge zum IT-Grundschutz der Stiftungsuniversität genügen.

(4) Für die Speicherung und Verarbeitung dienstlicher Daten auf privater Hardware ist A.16 zu beachten.

(5) Beim Verlust privater Hardware, auf der dienstliche Daten gespeichert wurden, ist die oder der ISK zu informieren.

A.19 Datensicherung und Archivierung

Verantwortlich für Initiierung:	Fachverantwortliche
Verantwortlich für Umsetzung:	IT-Personal, Fachverantwortliche

(1) Daten müssen vor Verlust durch Fehlbedienung, technische Störungen o. ä. geschützt werden. Dazu müssen regelmäßig Datensicherungen (Anlegen von Kopien der Daten auf getrennten Speichersystemen) durchgeführt werden.

(2) Ist die Speicherung auf zentralen Servern mit geregelter Datensicherung nicht möglich, sind die jeweiligen Fachverantwortlichen für die Sicherung der Daten selbst verantwortlich.

(3) Bei zentraler Datensicherung haben sich die Fachverantwortlichen über die jeweils geltenden Bestimmungen zu Rhythmus und Verfahrensweise für die Datensicherung zu informieren.

(4) Von der Datensicherung zum Schutz vor Verlust ist die zur Umsetzung der „Ordnung der Georg-August-Universität Göttingen zur Sicherung guter wissenschaftlicher Praxis“ nötige Langzeitarchivierung wissenschaftlicher Daten zu unterscheiden. Diese ist von den Fachverantwortlichen sicherzustellen.

A.20 Umgang mit Datenträgern

Verantwortlich für Initiierung:	Fachverantwortliche
Verantwortlich für Umsetzung:	Fachverantwortliche

(1) Datenträger sind an gesicherten Orten aufzubewahren. Erforderlichenfalls sind Datenträgertresore zu beschaffen.

(2) Weiterhin sind Datenträger zu kennzeichnen, sofern die Identifikation des Datenträgers nicht durch ein anderes technisches Verfahren erfolgt.

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

A.21 Löschen und Entsorgung von Datenträgern

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

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

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

(3) Weitere Informationen können bei folgenden Stellen erfragt werden: GWDG, Geschäftsbereich Informationstechnologie für die Universitätsmedizin, Abteilung IT für die Universitätsverwaltung, Datenschutzbeauftragte der Universität und der Universitätsmedizin.

A.22 Sichere Entsorgung vertraulicher Papiere

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

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

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

I. Maßnahmen für IT-Personal

I.1 Frühzeitige Berücksichtigung von Informationssicherheitsfragen

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

(1) Fragen der Informationssicherheit und des Datenschutzes müssen bei Neubeschaffungen von IT-Systemen und der Einführung oder wesentlichen Änderungen von IT-Verfahren bereits im Planungsstadium berücksichtigt werden.

(2) Soweit personenbezogene Daten verarbeitet werden, ist auch die oder der zuständige Datenschutzbeauftragte frühzeitig einzubinden.

I.2 Festlegung von Verantwortlichkeiten und Rollentrennung

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

(1) Für jedes IT-Verfahren sind die Verantwortlichkeiten eindeutig festzulegen. Bei allen administrativen Anwendungen, die gesetzlichen Anforderungen genügen müssen und Anwendungen, bei denen ein besonderer Schutzbedarf vorliegt, ist ein Rollenkonzept erforderlich.

(2) Jede Person ist über die ihr übertragenen Verantwortlichkeiten und die sie betreffenden Bestimmungen zu informieren.

I.3 Dokumentation und Beschreibung der IT-Verfahren

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

(1) Zur Gewährleistung der Informationssicherheit eines IT-Verfahrens ist eine Dokumentation und Beschreibung zu erstellen. Hierzu gehören insbesondere folgende Angaben:

(a) Aufgabe des Verfahrens

(b) Systemübersicht, Netzplan

(c) Schnittstellen zu anderen Verfahren

(d) Datenbeschreibung

(2) Zur Gewährleistung der Informationssicherheit eines IT-Verfahrens ist eine Dokumentation zu erstellen, die wenigstens die folgenden Punkte umfasst:

(a) Vertretungsregelungen, insbesondere im Administrationsbereich

(b) Zugriffsrechte

(c) Organisation, Verantwortlichkeit und Durchführung der Datensicherung

(d) Installation und Freigabe von Software einschließlich von Softwareaktualisierungen

(e) Zweck, Freigabe und Einsatz selbst erstellter Programme

(f) Dienstanweisungen

(g) Arbeitsanleitungen für Administrationsaufgaben u.ä.

(h) auftretende Informationssicherheits-Ereignisse aller Art

(i) Notfallregelungen

(j) Wartungsvereinbarungen

(k) Beschreibung von Verarbeitungstätigkeiten gem. Art. 30 DSGVO

I.4 Dokumentation von Informationssicherheitsereignissen und -vorfällen

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

(1) Informationssicherheitsereignisse und -vorfälle sind vom zuständigen IT-Personal zu dokumentieren und die oder dem ISK unverzüglich mitzuteilen.

I.5 Regelungen der Auftragsverarbeitung

Verantwortlich für Initiierung:	Fachverantwortliche
Verantwortlich für Umsetzung:	Fachverantwortliche

(1) Eine schriftliche Vereinbarung ist Voraussetzung für alle im Auftrag der Stiftungsuniversität Göttingen betriebenen IT-Verfahren. Es sind eindeutige Zuweisungen der Verantwortlichkeit für die Informationssicherheit und entsprechende Kontrollmöglichkeiten festzulegen.

(2) Sofern im Rahmen der Auftragsverarbeitung personenbezogene Daten verarbeitet werden, sind die Regelungen der DSGVO (insbesondere Art. 28) zu beachten. Der bzw. die Datenschutzbeauftragte der Universität Göttingen bzw. der Universitätsmedizin Göttingen ist einzubeziehen.

I.6 Standards für technische Ausstattung und Konfiguration

Verantwortlich für Initiierung:	CIO
Verantwortlich für Umsetzung:	Fachverantwortliche, IT-Personal

(1) Zur Erreichung eines angemessenen Sicherheitsniveaus für IT-Systeme ist eine Standardisierung der technischen Ausstattung und der Konfiguration anzustreben. Die oder der ISB und die zentralen IT-Dienstleister beraten die Betreiber der IT-Verfahren.

I.7 Bereitstellung zentraler IT-Dienste

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

(1) Zentrale IT-Dienste wie Nutzerservice, Datensicherungsmaßnahmen, Ablage von Daten auf zentralen Fileservern, Ausführung von Programmen auf Anwendungsservern, Softwareverteilung, -aktualisierung, -inventarisierung und -lizenzverwaltung, E-Mail unterstützen einen reibungslosen IT-Einsatz und verbessern das Informationssicherheitsniveau. Entsprechende Dienste sind möglichst zentral anzubieten.

(2) Maßnahmen zur Abwehr von Schadsoftware sind ebenfalls zu zentralisieren.

(3) Beim Einsatz netzwerkweit operierender Installations- und Inventarisierungswerkzeuge sowie für Fernzugriffe, z.B. des Nutzerservice, sind besondere Maßnahmen zum Schutz vor Missbrauch zu ergreifen. Die Anwender sind vor dem Einsatz solcher Werkzeuge zu informieren.

I.8 Nutzung zentraler Dienste

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	IT-Personal

(1) Durch die zentrale Bereitstellung wesentlicher IT-Dienste durch die IT-Dienstleister werden die Einrichtungen der Stiftungsuniversität Göttingen entlastet, um ihre eigentlichen Aufgaben besser erfüllen zu können. Durch eine Zentralisierung von IT-Diensten wird eine verbesserte Informationssicherheit erreicht.

(2) Die Einrichtungen der Stiftungsuniversität Göttingen sollen auf zentrale IT-Dienste der IT-Dienstleister zurückgreifen. Eigene IT-Systeme dürfen nur betrieben werden, wenn entsprechende zentrale IT-Dienste für die eigenen Aufgabenstellungen nicht zur Verfügung stehen.

I.9 Vertretung

Verantwortlich für Initiierung:	Zuständige Leitung / Fachverantwortliche
Verantwortlich für Umsetzung:	Zuständige Leitung

(1) Für alle von IT-Personal wahrgenommen Aufgaben sind Vertretungsregelungen erforderlich. Die Vertretungen müssen alle hierfür erforderlichen Tätigkeiten beherrschen; ihnen sollen Arbeitsanweisungen und Dokumentationen zur Verfügung gestellt werden.

(2) Die Vertretungsregelung muss im System abgebildet sein und darf nicht durch die Weitergabe von Passwörtern erfolgen. Hiervon ausgenommen sind systemspezifische, nicht personenbezogene Nutzerkonten (zum Beispiel root bei UNIX-Systemen). Dort soll der Vertreter nur im Bedarfsfall auf das an geeigneter Stelle hinterlegte Passwort des Nutzerkontos zurückgreifen können.

(3) Die Einhaltung von Anforderungen an die Rollentrennung ist sicherzustellen.

I.10 Qualifizierung

Verantwortlich für Initiierung:	Zuständige Leitung / Fachverantwortliche
Verantwortlich für Umsetzung:	Zuständige Leitung

(1) IT-Personal darf erst nach ausreichender Schulung mit IT-Verfahren arbeiten.

(2) Eine Schulung muss auch die geltenden Sicherheitsmaßnahmen, die rechtlichen Rahmenbedingungen sowie die Erfordernisse des Datenschutzes umfassen.

(3) Es ist sicherzustellen, dass die ständige Fortbildung des IT-Personals in allen ihr Aufgabengebiet betreffenden Belangen erfolgt.

I.11 Basismaßnahmen

Verantwortlich für Initiierung:	Gebäudemanagement / ISK
Verantwortlich für Umsetzung:	Gebäudemanagement

(1) Zur Sicherung der IT-Infrastruktur ist eine Vielzahl baulicher und technischer Vorgaben zu beachten. Technische Maßnahmen zur Infrastruktur sind beispielsweise im Grundschutzkompendium des BSI[4] beschrieben. Die Zuständigkeit für Brandschutz liegt bei der Feuerwehr und für die weitere Sicherheitsinfrastruktur

[4] Siehe https://www.bsi.bund.de/grundschutz

bei der Stabsstelle Sicherheitswesen/Umweltschutz der Universität. Folgende Maßnahmen zur Sicherung der IT-Infrastruktur sind zu beachten:

(a) Unterbrechungsfreie Stromversorgung (USV)

(b) Brandschutz

(c) Schutz vor Wasserschäden

(d) Geschützte Kabelverlegung

I.12 Sicherung der Serverräume

Verantwortlich für Initiierung:	ISK
Verantwortlich für Umsetzung:	Gebäudemanagement

(1) Alle IT-Systeme mit typischer Serverfunktion, einschließlich der Peripheriegeräte (Konsolen, externe Platten, Laufwerke u. ä.), sind in separaten, besonders gesicherten Räumen aufzustellen.

(2) Der Zugang Unbefugter zu diesen Räumen muss zuverlässig verhindert werden.

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

(4) Die Türen dürfen nur durch geeignete Schließsysteme zu öffnen sein und sollen selbsttätig schließen; verwendete Schlüssel müssen kopiergeschützt sein.

(5) 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.

(6) 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 und Türen, Bewegungsmelder o. ä., zur Verhinderung von gewaltsamen Eindringen vorzusehen.

(7) Eine Zentralisierung von Serverräumen ist anzustreben.

I.13 Sicherung der Netzknoten

Verantwortlich für Initiierung:	Gebäudemanagement / IT-Dienstleister
Verantwortlich für Umsetzung:	Gebäudemanagement

(1) Vernetzungsinfrastruktur (Switches, Router, 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 gesichert sind. Maßnahme I.12 gilt entsprechend.

I.14 Verkabelung und Funknetze

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	IT-Dienstleister, Gebäudemanagement, IT-Personal

(1) Die Netzwerkinfrastruktur ist klar zu strukturieren sowie aktuell und vollständig zu dokumentieren.

(2) Anträge auf Erweiterungen und Veränderungen an der Netzwerkinfrastruktur (beispielsweise Verkabelung, Netzwerkverteiler, Funknetze) sind mit der oder dem zuständigen ISK abzustimmen und bei den zuständigen zentralen Stellen

(Gebäudemanagement für die Universität, G3-7 für die Universitätsmedizin) einzureichen.

I.15 Einweisung und Beaufsichtigung von Fremdpersonal

Verantwortlich für Initiierung:	ISK
Verantwortlich für Umsetzung:	je nach Auftraggeber ISK, IT-Dienstleister, Gebäudemanagement

(1) Fremdpersonal, das in gesicherten Räumen mit IT-Ausstattung (z.B. Serverräume) Arbeiten auszuführen hat, muss beaufsichtigt und die Arbeiten müssen dokumentiert werden.

(2) Für regelmäßig eingesetztes und eingewiesenes Fremdpersonal kann auf eine Beaufsichtigung verzichtet werden. Die Ausnahmen sind zu dokumentieren.

(3) Fachfremde Personen (z.B. Reinigungspersonal), die Zugang zu gesicherten IT-Räumen benötigen, müssen über den Umgang mit IT-Ausstattung belehrt werden.

(4) Wenn bei Arbeiten durch Fremdpersonal, auch im Rahmen der Fernwartung, die Möglichkeit des Zugriffs auf schutzbedürftige Daten besteht, muss dieses auf das Datengeheimnis verpflichtet werden. Bei Zugriff auf personenbezogene Daten muss dieses auf das Datengeheimnis verpflichtet sein. Für die Wartung und Instandhaltung sind dann Verträge gemäß Art. 28 DSGVO abzuschließen.

I.16 Beschaffung, Softwareentwicklung

Verantwortlich für Initiierung:	ISK
Verantwortlich für Umsetzung:	Fachverantwortliche

(1) Die Beschaffung von Soft- und Hardware und die Entwicklung von Software sind mit der oder dem zuständigen ISK abzustimmen. Dabei sind die Standards gemäß I.6 und Sicherheitsmaßnahmen nach dem Stand der Technik zu beachten. Die fachlichen und technischen Anforderungen müssen vorher spezifiziert sein.

I.17 Kontrollierter Softwareeinsatz

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

(1) Auf IT-Systemen der Stiftungsuniversität Göttingen darf nur Software installiert werden, die zur Erfüllung der dienstlichen Aufgaben erforderlich ist.

(2) Das Einspielen von Software insbesondere 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 IT-Systeme oder das Datennetz ausgeht.

(3) Im Zweifelsfall ist die Zustimmung der zuständigen Leitung einzuholen. Sofern erforderlich steht die oder der ISB der Leitung beratend zur Seite.

I.18 Separate Entwicklungsumgebung

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

(1) Die Entwicklung oder Anpassung von insbesondere serverbasierter Software sollte nicht in der Produktionsumgebung erfolgen. Die Überführung der Software

von der Entwicklung in den Produktionsbetrieb bedarf der Freigabe durch den zuständigen Fachverantwortlichen.

I.19 Schutz vor Schadprogrammen

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

(1) Auf allen Arbeitsplatzrechnern ist grundsätzlich ein Virenscanner einzurichten, der automatisch alle eingehenden Daten und alle Dateien überprüft. Regelmäßig (möglichst automatisiert) ist der Virenscanner inkl. der Signaturen zu aktualisieren.

(2) Der Einsatz von Virenscannern ist für alle anderen IT-Systeme (z.B. Server, Mess- und Steuerrechner) zu prüfen und soweit technisch möglich vorzunehmen.

(3) Wird auf einem System schädlicher Programmcode entdeckt, muss dies der zuständigen oder dem zuständigen ISK gemeldet und das Ergebnis der eingeleiteten Maßnahmen dokumentiert werden.

(4) In regelmäßigen Abständen sowie bei konkretem Bedarf oder Verdacht ist eine Suche nach Schadprogrammen auf allen bedrohten IT-Systemen vorzunehmen; die Ergebnisse sind zu dokumentieren.

(5) Von Herstellern bereitgestellte Softwareaktualisierungen zur Beseitigung von Sicherheitslücken sind zeitnah einzuspielen, soweit keine Probleme mit der Aktualisierung erkennbar sind.

(6) Betriebssysteme und Anwendungen, die vom Hersteller nicht mehr mit Softwareaktualisierungen versorgt werden, dürfen grundsätzlich nicht mehr am Datennetz betrieben werden. Ist ein Weiterbetrieb solcher Systeme aus übergeordneten Gründen unumgänglich, sind diese Systeme zu dokumentieren, spezifische Informationssicherheitskonzepte für einen Weiterbetrieb zu entwickeln und zur Stellungnahme der oder dem ISB vorzulegen.

(7) Anwendungen – insbesondere Netzanwendungen wie Mailprogramme und WWW-Browser – sind sicher zu konfigurieren.

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

I.20 Schnittstellen für externe Datenträger bei erhöhtem Schutzbedarf

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

(1) Bei entsprechend erhöhtem Schutzbedarf müssen alle äußeren Zugänge des PCs (zum Beispiel CD-Laufwerke, USB-Anschlüsse, Wechseldatenträger, kabellose Verbindungen) entfernt, gesperrt oder kontrolliert werden, wenn sie für die dienstlichen Aufgaben nicht erforderlich sind. Die Möglichkeit der Nutzung von Anwendungsservern und laufwerkslosen Arbeitsplatzrechnern oder Terminals ist zu prüfen.

(2) Der Zugriff auf das Rechner-BIOS ist durch ein Passwort zu schützen.

I.21 Ausfallsicherheit

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

(1) Maßnahmen zur Ausfallsicherheit sind entsprechend der jeweiligen Anforderung zu ergreifen.

(2) IT-Systeme, die zur Aufrechterhaltung eines geordneten Betriebs notwendig sind, müssen durch Ausweichlösungen (z.B. durch redundante Geräteauslegung oder Übernahme durch gleichartige Geräte) oder Wartungsverträge mit kurzen Reaktionszeiten hinreichend verfügbar gehalten werden.

I.22 Einsatz von Diebstahl-Sicherungen

Verantwortlich für Initiierung:	ISK
Verantwortlich für Umsetzung:	Gebäudemanagement, IT-Personal

(1) Zur Reduzierung des Diebstahlrisikos sind Diebstahl-Sicherungen überall dort einzusetzen, wo nicht unwesentliche Werte zu schützen sind und andere Maßnahmen (z. B. geeignete Zutrittskontrolle zu den Arbeitsplätzen (s. A.6)) nicht umgesetzt werden können oder ein besonderes Diebstahlsrisiko (z. B. durch Publikumsverkehr oder die Fluktuation von Nutzern) existiert.

(2) Datenträger mit wertvollen Forschungsdaten und personenbezogenen Daten sind in angemessener Weise zu schützen.

I.23 Personenbezogene Nutzerkonten (Authentisierung)

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

(1) Zusätzlich zu Maßnahme A.9 ist zu beachten:

(2) Jeder Person sollte nur ein Nutzerkonto zugeordnet sein. Die Zuordnung von mehreren Nutzerkonten zu einer Person innerhalb eines IT-Systems sollte nur in begründeten Ausnahmefällen erlaubt sein, wie beispielsweise für Systemadministratoren.

(3) Die Einrichtung und Freigabe eines Nutzerkontos darf nur in einem geregelten Verfahren erfolgen. Die Einrichtung und Freigabe ist zu dokumentieren.

(4) Vorinstallierte Standardkonten sind soweit nicht benötigt zu deaktivieren oder zu löschen.

I.24 Administratorkonten

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

(1) Die Administratoren erhalten für ihre Aufgaben ein persönliches Administratorkonto. Das Nutzen dieses Administratorkontos muss auf die Aufgaben beschränkt bleiben, für die Administrationsrechte notwendig sind. Für die nicht-administrative Tätigkeiten sind Nutzerkonten ohne Administrationsrechte zu verwenden.

(2) Vordefinierte Administratorkonten sind soweit technisch möglich umzubenennen, damit deren Bedeutung nicht sofort ersichtlich ist.

I.25 Verwaltung von Nutzerkonten bei Eintritt, Wechsel, Ausscheiden

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	Zuständige Leitung, Vorgesetzter der ausscheidenden Person

(1) Im organisatorischen Ablauf muss ein Prozess für die Verwaltung von Nutzerkonten und Nutzerrechten bei Eintritt, organisatorischem Wechsel und Ausscheiden von Personen zuverlässig festgelegt sein.

(2) Beim organisatorischen Wechsel oder Ausscheiden von Personen hat die zuständige Leitung über die Verwendung der dienstlichen Daten zu entscheiden, die dem Nutzerkonto der Person zugeordnet sind.

(3) Es sind sämtliche für die wechselnde oder ausscheidende Person eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen oder zu löschen.

(4) Wurden in Ausnahmefällen Nutzerkonten zu einem IT-System zwischen mehreren Personen geteilt, so ist nach dem Wechsel oder Ausscheiden einer der Personen das Passwort zu ändern.

I.26 Passwörter

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

(1) Neben den Bestimmungen der Ziffer A.12 ist zusätzlich von IT-Personal zu beachten:

(a) Für privilegierte Konten sind erhöhte Anforderungen an die Passwortstärke (Komplexität und/oder Länge des Passworts) zu stellen.

(b) Voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen) müssen unverzüglich durch individuelle Passwörter ersetzt werden.

(2) Sofern technisch umsetzbar, sind folgende Rahmenvorgaben einzuhalten:

(a) Die technischen Möglichkeiten zur Erzwingung der Einhaltung von Passwortrichtlinien müssen aktiviert werden.

(b) Jede Nutzerin und jeder Nutzer muss sein eigenes Passwort jederzeit ändern können.

(c) Für die Erstanmeldung neuer Nutzerinnen und Nutzer müssen Passwörter vergeben werden, die nach einmaligem Gebrauch gewechselt werden müssen.

(d) Die Anzahl von fehlerhaften Anmeldeversuchen an ein System innerhalb eines Zeitraums muss begrenzt werden. Dies kann durch eine Sperrung erfolgen, die entweder nur vom Systemadministrator aufgehoben werden kann oder zeitlich befristet ist, oder durch andere Algorithmen, die die Anzahl der Anmeldeversuche begrenzen.

(e) Bei der Authentisierung in vernetzten Systemen dürfen Passwörter grundsätzlich nur verschlüsselt übertragen werden. In Netzen, in denen Passwörter unverschlüsselt übertragen werden müssen, erfolgt ausschließlich die Verwendung von Einmalpasswörtern.

(f) Bei der Eingabe darf das Passwort nicht auf dem Bildschirm angezeigt werden.

(g) Die Passwörter müssen im System sicher gespeichert werden, z. B. mittels Einwegverschlüsselung.

(h) Der Passwortwechsel muss vom System entsprechend den Regeln für den Passwortwechsel regelmäßig initiiert werden.

(i) Die Wiederholung alter Passwörter beim Passwortwechsel muss vom IT-System verhindert werden (Passwort-Historie).

(3) Ist es nicht möglich, die Einhaltung der Passwortrichtlinien systemintern zu erzwingen, so sind geeignete organisatorische Maßnahmen zu ergreifen, um Nutzerinnen und Nutzer auf die Passwortrichtlinien hinzuweisen und auf deren Einhaltung zu verpflichten.

(4) Abweichungen von den in Sätzen (1) und (2) genannten Regeln sind nur für Systeme zulässig, für die eine besondere Passwort-Richtlinie dies ausdrücklich erlaubt.

(5) Der Einsatz von Alternativen und Erweiterungen (Zwei-Faktor-Verfahren) zur Authentifizierung mittels Passwörtern ist insbesondere dort durch das IT-Personal zu prüfen, wo über solche Verfahren ein erhöhter Schutzbedarf gewährleistet werden soll oder muss.

I.27 Zugriffsrechte

Verantwortlich für Initiierung:	Zuständige Leitung, ISK
Verantwortlich für Umsetzung:	IT-Personal

(1) Über Zugriffsrechte wird festgelegt, welche Person im Rahmen ihrer Funktionen bevollmächtigt wird, IT-Systeme, IT-Anwendungen oder Daten zu nutzen. Der Nutzerinnen und Nutzer dürfen nur mit den Zugriffsrechten arbeiten, die für die Erfüllung ihrer Aufgaben vorgesehen sind.

(2) Die Verfahren zur Vergabe von Zugriffsrechten sowie die Dokumentation der Vergabe und der Rechte sind technisch und organisatorisch festzulegen.

(3) Es ist zu prüfen, inwieweit die Zugriffserlaubnis auf bestimmte Endgeräte begrenzt werden kann.

(4) Es ist ebenfalls zu prüfen, inwieweit die Zugriffserlaubnis auf bestimmte Zeiten begrenzt werden kann oder muss (z. B. Beschränkung auf die üblichen Arbeitszeiten).

(5) Für Nutzerinnen und Nutzer mit privilegierten Rechten, insbesondere für Administratorkonten, ist der Zugriff auf die benötigten Systeme (i.d.R. sind es der betreffende Server und Endgeräte oder Anwendungen) zu begrenzen.

(6) Bei allen administrativen Anwendungen, die gesetzlichen Anforderungen genügen müssen (Datenschutz, Handelsgesetzbuch, u.a.), erfolgt die Vergabe und Änderung der Zugriffsrechte für die einzelnen Nutzerinnen und Nutzer auf deren schriftlichen Antrag. Dabei ist bei der Vergabe von Zugriffsrechten die Funktionstrennung zu beachten; Administratoren dürfen sich nicht selbst verwalten.

I.28 Sperren, abmelden und ausschalten

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

(1) Zusätzlich zu A.6 gilt:

(2) Soweit technisch umsetzbar ist die Aktivierung automatischer Sperrungen zentral zu konfigurieren.

I.29 Telearbeit

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

(1) Zusätzlich zu A.13 gilt:

(2) Durch entsprechende technische Maßnahmen ist sicherzustellen, dass

(a) bei der Kommunikation zwischen Telearbeitsplatz und Dienststelle die Vertraulichkeit und die Integrität der übertragenen Daten gewährleistet sind,

(b) nur Berechtigte von zu Hause aus auf dienstliche Daten zugreifen können,

(c) dienstliche Daten am Telearbeitsplatz vertraulich behandelt werden und

(d) das gesamte Verfahren der Telearbeit revisionssicher ist.

(3) Zur Einrichtung und zum Betrieb von Telearbeitsplätzen sind die bestehenden Dienstvereinbarungen[5] zu beachten.

(4) Werden bei der Telearbeit personenbezogene Daten verarbeitet, muss die bzw. der zuständige Datenschutzbeauftragte am Genehmigungsprozess beteiligt werden.

I.30 Notwendigkeit von Protokollierung und Monitoring

Verantwortlich für Initiierung:	ISK / Fachverantwortliche
Verantwortlich für Umsetzung:	IT-Personal

(1) Eine angemessene Protokollierung, Auditierung und Revision sind wesentliche Faktoren der Informationssicherheit. Eine Auswertung solcher Protokolle mit geeigneten Hilfsmitteln erlaubt beispielsweise einen Rückschluss darauf, ob die Bandbreite des Netzes den derzeitigen Anforderungen entspricht oder systematische Angriffe auf das Netz zu erkennen sind.

(2) Je nach Einsatz eines IT-Verfahrens müssen adäquate Maßnahmen zur Protokollierung getroffen werden, um Datensicherheit, Datenschutz und Revisionsfähigkeit zu gewährleisten.

(3) Die Auswertung von Protokolldateien ist in Abhängigkeit mit den protokollierten Daten mit den Datenschutzbeauftragten, dem Personalrat und der Internen Revision abzustimmen.

[5] s. Anlage Mitgeltende Dokumente

I.31 Protokollierung auf Servern und bei Anwendungsprogrammen

Verantwortlich für Initiierung:	ISK / Fachverantwortliche
Verantwortlich für Umsetzung:	IT-Personal

(1) Je nach den Möglichkeiten des Betriebssystems, der Dienste und der Anwendungen sind alle Zugangsversuche, sowohl die erfolgreichen als auch die erfolglosen, automatisch zu protokollieren.

(2) Das Ändern der Parameter von Systemdiensten und Anwendungsprogrammen, das Herunter – und Hochfahren des IT-Systems oder von Systemdiensten sowie sicherheitsrelevante Ereignisse sind zu protokollieren.

(3) Das Prinzip der Zweckbindung nach Art. 5 Abs. 1 lit. b) DSGVO und der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c) DSGVO sind zu beachten.

(4) Die Protokolle sind, sofern technisch möglich, auf dafür dedizierten Servern zu speichern.

(5) Die Protokolle sind regelmäßig und unverzüglich nach Erstellung auszuwerten. Es muss dabei sichergestellt sein, dass nur die Personen Zugriff auf die Protokolle erlangen, die diesen für die Erledigung der ihnen durch die zuständige Stelle zugewiesenen Aufgaben benötigen.

I.32 Protokollierung der Administrationstätigkeit

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

(1) Die Administratoren sind durch organisatorische Regelungen (Dienstanweisungen o.ä.) je nach Schutzbedarf des Verfahrens oder der zu verarbeitenden Daten zu verpflichten, die im Rahmen ihrer Aufgaben durchgeführten Tätigkeiten zu protokollieren. Soweit möglich sollte die Protokollierung automatisch im System erfolgen.

I.33 Sichere Netzwerkadministration

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

(1) Es muss in Betriebs- und Sicherheitskonzepten geregelt werden und sichergestellt sein, dass die Administration des Netzwerks nur von dem dafür vorgesehenen IT-Personal durchgeführt wird.

(2) Aktive und passive Netzkomponenten sowie Server sind vor dem Zugriff Unbefugter zu schützen.

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

I.34 Netzmonitoring

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

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

(2) Es muss in Betriebs- und Sicherheitskonzepten geregelt sein und überprüft werden, dass auf die für diesen Zweck eingesetzten Werkzeuge und Daten nur die dafür berechtigten Personen zugreifen können.

(3) Der Kreis der berechtigten Personen ist auf das erforderliche Maß zu beschränken.

I.35 Kontrollierte Netzwerkzugänge

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

(1) Unberechtigte Nutzung von Netzwerkzugängen ist durch organisatorische und technische Maßnahmen zu unterbinden.

I.36 Aufteilungen in Bereiche unterschiedlichen Schutzbedarfs

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

(1) Das Datennetz ist so zu strukturieren, dass Teilnetze für verschiedene IT-Systeme entsprechend ihres jeweiligen Schutzbedarfs bereitgestellt werden.

(2) IT-Systeme mit unterschiedlichem Schutzbedarf dürfen nicht in gleichen Teilnetzen betrieben werden. Dadurch wird verhindert, dass IT-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 IT-Systemen mit geringerem Schutzbedarf nicht unnötig erschwert wird, weil auf andere IT-Systeme mit höherem Schutzbedarf im gleichen Teilnetz Rücksicht genommen werden muss.

I.37 Kontrollierte Kommunikationskanäle

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

(1) Die gesamte Kommunikation zwischen verschiedenen Teilnetzen der Stiftungsuniversität Göttingen oder mit Externen darf ausschließlich über kontrollierte Kanäle erfolgen, die durch spezielle Schutzsysteme (Firewall, Proxy o.ä.) geführt werden.

(2) Schutzsysteme sind so zu konfigurieren, dass nur erwünschte Kommunikationen möglich sind (Whitelisting) und damit unnötige Kommunikationen unterbunden werden und Angriffsflächen minimiert werden.

(3) Neben den Netzverbindungen der Stiftungsuniversität Göttingen sind die Installation und der Betrieb anderer Kommunikationsverbindungen grundsätzlich nicht gestattet. Sofern auf Grund besonderer Umstände die Installation anderer Kommunikationswege unumgänglich ist (z.B. der Betrieb eines Modems zu Fernwartungszwecken), bedarf dies zuvor der Genehmigung durch die Netzbetreiber. Für Zugriffe externer Dienstleister ist I.15 zu beachten.

I.38 Gesicherte Übertragungsverfahren

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

(1) Für die elektronische Kommunikation sind, soweit technisch umsetzbar, verschlüsselte Übertragungsverfahren einzusetzen.

(2) Schützenswerte Daten sind zwingend verschlüsselt zu übertragen.

(3) Für Administrationstätigkeiten und Fernwartungen sind zwingend verschlüsselte Übertragungsverfahren einzusetzen.

I.39 Organisation der Datensicherung

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

(1) Die Datensicherung muss nach einem dokumentierten Datensicherungskonzept erfolgen, das dem Schutzbedarf der zu sichernden Daten angemessen ist. Das Datensicherungskonzept umfasst alle Regelungen der Datensicherung (was wird von wem nach welcher Methode, wann, wie oft und wo gesichert).

(2) Im Falle personenbezogener Daten sind die geforderten bzw. erlaubten Aufbewahrungsfristen zu beachten.

(3) Originaldaten und Sicherungskopien sind in unterschiedlichen Brandabschnitten aufzubewahren.

(4) Daten sind grundsätzlich auf zentralen Fileservern zu speichern, bei denen turnusmäßig eine zentrale Datensicherung durchgeführt wird. Sofern eine Speicherung auf zentralen Fileservern derzeit nicht möglich ist, muss für das lokale System eine geeignete Datensicherung eingerichtet werden.

(5) Unter dem Aspekt möglichst geringer Wiederherstellungszeiten ist zu prüfen, inwieweit neben Daten auch System- und Programmbereiche gesichert werden.

(6) Die Konfigurationen aller aktiven Netzkomponenten sind in eine regelmäßige, mindestens tägliche Datensicherung einzubeziehen.

I.40 Anwenderinformation zur Datensicherung

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

(1) Alle Anwender, die Datensicherungssysteme nutzen können, sind über die Bestimmungen zur Datensicherung zu informieren, um erforderlichenfalls auf Unzulänglichkeiten (z.B. ungeeignetes Zeitintervall für ihren Bedarf) hinweisen oder individuelle Ergänzungen vornehmen zu können.

I.41 Verifizierung der Datensicherung

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

(1) Die Konsistenz der Datensicherungsläufe ist sicherzustellen, indem die Lesbarkeit der Datensicherung überprüft wird. Das testweise Wiedereinspielen von Datensicherungen soll wenigstens einmal jährlich erfolgen.

I.42 Löschen und Entsorgen von Datenträgern

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

(1) Zusätzlich zu A.21 gilt:

(2) Die Reparatur beschädigter Datenträger, auf denen schützenswerte Daten gespeichert sind, ist nur in besonders begründeten Ausnahmenfällen erlaubt.

(3) Wenn Datenträger nur durch externe Dienstleister repariert werden können, ist der Auftragnehmer auf die Wahrung der Vertraulichkeit der Daten zu verpflichten. Die Verpflichtung muss Bestandteil der schriftlichen Vereinbarung sein.

I.43 Sichere Entsorgung vertraulicher Unterlagen

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

(1) Zusätzlich zu A.22 gilt:

(2) Bei der Beschaffung eines Aktenvernichters ist die DIN 66399 zu beachten.

(3) Bei einer Entsorgung über einen Dienstleister muss sichergestellt sein, dass der Auftragnehmer entsprechend zertifiziert ist. Der Auftragnehmer ist zur Protokollierung der Vernichtung zu verpflichten.

Anlage 3 Glossar

Anwendung

Ein Computerprogramm oder eine Menge zusammenwirkender Computerprogramme, mit dem oder mit denen IT-Verfahren abgearbeitet werden.

Anwendungsserver

Ein Server, auf dem Anwendungen (anstelle eines Arbeitsplatzrechners) ausgeführt werden.

Datenbestand

Eine Menge von digital gespeicherten Daten.

Datenarchivierung

Ist die Datenspeicherung in einem System, das zur langfristigen Aufbewahrung von Datenbeständen vorgesehen ist.

Datenarchivierung erfordert insbesondere bei Forschungsdaten die Speicherung zusätzlicher Daten (Metadaten) zur Beschreibung des Dateninhalts und Datenformats.

Datensicherung

Erstellung von zusätzlichen Kopien von Daten auf getrennten Datenträgern zum Schutz vor Verlust der Daten durch Hardwareschäden oder vor versehentlichem Löschen.

Datensicherungen schützen i.d.R. vor Verlust durch versehentliches Löschen nur für eine begrenzte Zeit, da Datensicherungsverfahren i.d.R. Kopien gelöschter Daten nach einer vordefinierten Zeit auch auf dem Datensicherungsdatenträger löschen.

Datenspeicherung

Ist der Vorgang, bei dem Daten auf einen Datenträger geschrieben werden.

Datenträger

Medien, auf denen Daten gespeichert werden, z.B. Festplatten, Disketten, USB-Sticks, Speicherkarten.

Gefahr

a) Gegenwärtige Gefahr:

Eine Gefahr, bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzenden Wahrscheinlichkeit bevorsteht.

b) Erhebliche Gefahr:

Eine Gefahr für ein bedeutsames Rechtsgut wie Leben, Gesundheit, Freiheit, nicht unwesentliche Vermögenswerte sowie andere strafrechtlich geschützte Güter.

Informationssicherheitsereignisse

(Nach ISO27000) Erkanntes Auftreten eines System-, Service- oder Netzwerkzustands, der einen möglichen Verstoß gegen die Informationssicherheitsrichtlinie, das Versagen von Maßnahmen oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte, anzeigt.

Informationssicherheitsvorfälle

(Nach ISO27000) Einzelne oder eine Reihe von unerwünschten oder unerwarteten Informationssicherheitsereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die Informationssicherheit bedroht wird.

Initiierung

Unter „Verantwortlich für die Initiierung“ wird im Maßnahmenkatalog für den IT-Grundschutz festlegt, welche Person für den Beginn und die Umsetzung einer Maßnahme verantwortlich ist.

IT-Anwenderinnen und IT-Anwender

Nutzerinnen und Nutzer eines IT-Systems mit einem nicht privilegierten Nutzerkonto, die oder der lediglich von anderen Stellen bereitgestellte Rechner, Betriebssysteme und Anwendungen zur Verarbeitung deren oder dessen Daten und zur Erledigung deren oder dessen Aufgaben benutzt.

IT-Personal

IT-Personal sind alle Mitglieder der Stiftungsuniversität Göttingen, die mit der Wahrnehmung von Aufgaben in der Planung, Betreuung, Pflege und Administration von IT-Systemen beauftragt sind, die über die bloße Nutzung der IT-Systeme hinausgehen. Dabei ist unerheblich, ob diese Personen diese Tätigkeiten hauptberuflich wahrnehmen. Insbesondere gelten alle Personen mit Rechten zur Veränderung der Installation von Betriebssystemen und Anwendungen auf IT-Systemen als IT-Personal.

IT-System

Unter IT-System oder informationstechnischem System versteht man elektronische datenverarbeitende Systeme. Darunter fallen jegliche Computer vom Smartphone bis zum Großrechner, aber auch Zusammenschlüsse von einzelnen Geräten zu einem zusammengesetzten System zur gemeinsamen Datenverarbeitung.

IT-Verfahren

Definiertes Verfahren zur elektronischen Datenverarbeitung inkl. elektronischer Kommunikation.

Netzbetreiber

Von der Stiftungsuniversität Göttingen mit der Installation und dem Betrieb von Datennetzen betraute Einrichtungen und deren Mitarbeiter. In der Stiftungsuniversität Göttingen sind dies die GWDG für die Universität und der Geschäftsbereich Informationstechnologie für die UMG.

Nutzerinnen und Nutzer

Personen, die ein IT-System zur elektronischen Datenverarbeitung nutzen.

Nutzerkennung

Die einer Nutzerin oder einem Nutzer in einem IT-System zugeordnete Bezeichnung.

Nutzerkonto

Eine Repräsentation einer Nutzerin oder eines Nutzers innerhalb eines IT-Systems, die i.d.R. mit einer Nutzerkennung und Zugangsdaten zum System verbunden ist und über die Objekte und Rechte im IT-System der Nutzerin oder dem Nutzer zugeordnet werden können.

Nutzerkonto, privilegiertes

Spezielles Nutzerkonto, mit dem erhöhte Rechte im IT-System verbunden sind. Insbesondere werden darunter auch Nutzerkonten verstanden, die Rechte zur Installation oder Veränderung des Betriebssystems oder von Anwendungen haben.

Risikoakzeptanz

(Nach ISO 27000) Fundierte Entscheidung ein bestimmtes Risiko zu tragen

Risikominderung

Minderung von Risiken durch Maßnahmen, welche die Eintrittswahrscheinlichkeit oder Schadenshöhe verringern.

Risikoübertragung

Übertragung von Risiken auf Andere (z.B. durch Versicherungen).

Risikovermeidung

(Nach ISO 27000) Vermeiden des Risikos, indem entschieden wird, die Tätigkeit, die Anlass zu dem Risiko gibt, nicht zu beginnen oder fortzusetzen.

Schützenswerte Daten

Schützenswerte Daten im Sinne dieser Informationssicherheitsrichtlinie sind insbesondere

- personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO (z. B. Studierendendaten, Personaldaten, Patientendaten),
- Unternehmensdaten (z.B. Finanzdaten, vertrauliche interne Informationen/Protokolle),
- Patente sowie
- im Einzelfall weitere Daten, die von einer IT-Anwenderin oder einem IT-Anwender als schützenswerte Daten eingestuft wurden (z. B. Forschungsergebnisse).

Übertragung von Daten

Kopiervorgänge über Datennetze von einem IT-System zu einem anderen IT-System.

Zugangsdaten

Informationen, mit deren Hilfe die Identität einer Nutzerin oder eines Nutzers beim Zugang zu seinem Nutzerkonto überprüft wird, z.B. Passwörter und PINs, kryptographische Schlüssel oder biometrische Daten.

Studierendenschaft:

Das Studierendenparlament der Georg-August-Universität Göttingen hat am 16.12.2019 die siebte Änderung der Organisationssatzung der Studierendenschaft der Georg-August-Universität Göttingen (OrgS) in der Fassung der Bekanntmachung vom 30.03.2004 (Amtliche Mitteilungen 3/2004, S. 216), zuletzt geändert durch Beschlüsse des Studierendenparlaments vom 01.02.2018, 28.02.2018, 21.11.2018 und 17.12.2018 (Amtliche Mitteilungen I 9/2019 S. 77), beschlossen (§ 20 Abs. 2 Satz 1 NHG; § 14 Abs. 1 Buchstabe e), § 61 OrgS).

Die Änderung wird nachfolgend bekannt gemacht:

Artikel 1

Die Organisationssatzung der Studierendenschaft wird wie folgt geändert:

1. Nach § 60 wird als neuer Abschnitt VII Folgendes eingefügt:

„Abschnitt VII
Datenschutz

§ 61 Datenverarbeitung in der Studierendenschaft

(1) Alle Organe der Studierendenschaft verpflichten sich zum verantwortungsvollen Umgang mit allen personenbezogenen Daten.
(2) Die Rechte und Pflichten der Fachschaften in Bezug auf die Verarbeitung von personenbezogenen Daten richten sich nach den allgemeinen Vorschriften zur Fachschaft.

§ 62 Datenschutzbeauftragter oder Datenschutzbeauftragte

(1) Das Studierendenparlament wählt eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten der Studierendenschaft.
(2) Die Aufgaben der oder des Datenschutzbeauftragten der Studierendenschaft entsprechen den üblichen gesetzlichen Rechten und Pflichten einer oder eines Datenschutzbeauftragten für öffentliche Stellen.
(3) [1]Die oder der Datenschutzbeauftragte unterliegt nicht den Weisungen der Studierendenschaft und ihren Organen. [2]Umgekehrt ist die oder der Datenschutzbeauftragte aber auch nicht weisungsbefugt gegenüber der Studierendenschaft und ihren Organen.
(4) Die oder der Datenschutzbeauftragte der Studierendenschaft wird bis auf Widerruf oder Rücktritt gewählt.

§ 63 Datenschutzmanager oder Datenschutzmanagerin

(1) Ein Fachschaftsparlament darf jeweils eine Datenschutzmanagerin oder einen Datenschutzmanager für seine Fachschaft wählen.
(2) Die Datenschutzmanagerin oder der Datenschutzmanager einer Fachschaft fungiert im Innenverhältnis als Kontaktperson gegenüber der oder dem Datenschutzbeauftragten der Studierendenschaft.
(3) Die Datenschutzmanagerin oder der Datenschutzmanager einer Fachschaft wird bis auf Widerruf oder Rücktritt gewählt.

§ 64 Auftragsverarbeitung

(1) Der AStA unterzeichnet Auftragsverarbeitungsvereinbarungen.
(2) Auf Anfrage einer Fachschaft unterzeichnet der AStA nach Beratung mit der oder dem Datenschutzbeauftragten der Studierendenschaft eine Auftragsverarbeitungsvereinbarung, insofern keine sachlichen Gründe dagegensprechen.
(3) Die Organe der Studierendenschaft haben vorrangig die Dienste bestehender Auftragsverarbeiter zu nutzen.

§ 65 Dokumentation

(1) Der AStA hält hochschulöffentlich eine Liste aller vorhandenen Datenschutzmanagerinnen und Datenschutzmanager der Fachschaften sowie eine Liste aller Auftragsverarbeiter vor.
(2) Der AStA dokumentiert zusätzlich dauerhaft alle Verarbeitungsverzeichnisse und alle Datenschutz-Folgeabschätzungen.

§ 66 Veränderungen

Über Änderungen des Abschnitts VII „Datenschutz“ entscheidet das Studierendenparlament nach Stellungnahme der oder des Datenschutzbeauftragten der Studierendenschaft, die wenigstens in Textform vorliegen muss.“

2. Der bisherige „Abschnitt VII Übergangs- und Schlussbestimmungen“ wird zu Abschnitt VIII und die bisherigen §§ 61 bis 64 werden zu §§ 67 bis 70.

Artikel 2

Die Änderung tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Mitteilungen I der Georg-August-Universität Göttingen in Kraft.