Aktuelle Fassung vom 09.05.2025
(Amtliche Mitteilungen I Nr. 17 vom 08.05.2025 S. 312).

Nichtamtliche Lesefassung

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 Verantwortungsstrukturen, Aufgabenzuordnung, Zusammenarbeit der Beteiligten und inhaltliche Festlegungen im hochschulweiten Informationssicherheitsprozess sowie im Informationssicherheits-Risikomanagement (Anlage 3) 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 und deren Auswirkungen 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 und Informationssicherheits-Risikomanagement

(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) Der Schutzbedarf aller Informationen ist entsprechend der Kategorien normal, hoch und sehr hoch zu bestimmen; 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.

(4) Anlage 3 enthält ergänzende Vorgaben zum Informationssicherheit-Risikomanagement einschließlich der Aufgabenzuordnung, der Festlegung von Kriterien für die Bewertung des Schutzbedarfs, der Schadensauswirkungen, der Eintrittswahrscheinlichkeiten und der Risikoklassen.

(5) Bei Feststellung eines „normalen Schutzbedarfs“, ist bei Umsetzung der Maßnahmen gemäß Anlage 2 eine weitere Risikoanalyse nicht erforderlich.

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). Die Gesamtverantwortung schließt die Verantwortung für das Informationssicherheits-Risikomanagement ein; ergänzende Vorgaben zum Informationssicherheit-Risikomanagement enthält Anlage 3.

(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.

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

§ 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 Betriebskonzepte nach Absatz (6),

d) Entscheidung über die weitere Behandlung von Informationssicherheitsvorfällen nach § 17,

e) die Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß Anlage 3.

(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 Informationswerten, 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 Betriebskonzepte einschließlich der nach Überprüfungen überarbeiteten Fassungen 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 Betriebskonzepten,
   (e) unverzügliche Vorlage der Betriebskonzepte gegenüber der oder dem ISB,
   (f) Sammlung und Zurverfügungstellung der Betriebskonzepte der jeweiligen Einheit,
   (g) Bewertung der Schwere gemeldeter Informationssicherheitsvorfälle; Prüfung, ob eine Informationssicherheitsvorfall gleichzeitig auch eine Datenschutzvorfall sein könnte und Erstellung einer Handlungsempfehlung gemäß § 17 für die zuständige Leitung,
   (h) Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß Anlage 3.

(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 Informationswerten, Datenbeständen, IT-Verfahren, IT-Systeme und Infrastrukturen für die Umsetzung des Informationssicherheitsprozesses verantwortlich, was insbesondere die folgenden Aufgaben umfasst:
   (a) Feststellung des Schutzbedarfs von Informationswerten, Datenbeständen, IT-Verfahren, IT-Systemen und Infrastrukturen sowie Analysierung der Risiken,
   (b) Erstellung und Fortschreibung der Betriebskonzepte auf Basis von Schutzbedarfsfeststellung und Risikoanalyse,
   (c) regelmäßige Überprüfung der Schutzbedarfsfeststellung, Risikoanalyse und des Betriebskonzepts entsprechend der im Betriebskonzept festzulegenden Intervallen, wobei im Bereich der von der UMG betriebenen Kritischen Infrastruktur mindestens jährliche Intervalle festzulegen sind,
   (d) Veranlassung und Kontrolle der Umsetzung der Maßnahmen des Betriebskonzepts einschließlich des Risikobehandlungsplans, insbesondere auch bei Inanspruchnahme externer IT-Dienstleister (z.B. Auftragsverarbeitung).

(2) Den Fachverantwortlichen obliegt zudem die Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß Anlage 3.

(3) 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.

(4) 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 Betriebskonzepten auf Grund von Sicherheitsvorfällen (im Sinne von § 17 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 Betriebskonzepten.

(d) Zustimmung zu den Betriebskonzepten der Einheiten einschließlich der nach Überprüfung durch die Fachverantwortlichen überarbeiteten Fassungen; im Dissensfall entscheidet das Präsidium beziehungsweise der Vorstand,

(e) Erstellung und Aktualisierung eines Verzeichnisses aller Betriebskonzepte,

(f) Bewertung von Informationssicherheitsvorfällen und Ableitung von strukturellen und konzeptionellen Empfehlungen gemäß § 17,

(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.

(h) Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß Anlage 3.

(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 § 17 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,

(d) Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß Anlage 3.

§ 13 Datenschutz- und Informationssicherheits-Beirat (DIB)

(1) Der 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) der oder dem CIO der Universität und UMG,

(g) der Leiterin oder dem Leiter der Stabsstelle Revision,

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

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

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

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

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

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

(2) Für jedes Mitglied nach Absatz 1 ist eine Stellvertretung zu benennen.

(3) 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.

(4) Der 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) Empfehlung von Änderungsvorschlägen zur Informationssicherheitsrichtlinie und übergreifender Konzepte und Empfehlungen zur Informationssicherheit und zum Datenschutz.

(5) Dem DIB obliegt zudem die Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß Anlage 3.

§ 14 Externe Dienstleister

(1) 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.

(2) Die Einhaltung der Informationssicherheitsrichtlinie durch die externen IT-Dienstleister ist durch das zuständige IT-Personal des Auftraggebers zu überprüfen.

(3) Externe IT-Dienstleister sind darauf zu verpflichten, die Auftraggeber auf Risiken, die durch die von ihnen erbrachten Dienstleistungen im IT-System entstehen, hinzuweisen.

Abschnitt III: Inhaltliche Festlegungen

§ 15 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 Betriebskonzepten 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.

§ 16 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 erhöhter Schutzbedarf festgestellt, so sind zusätzliche Maßnahmen im Rahmen eines Betriebskonzepts von den Fachverantwortlichen festzulegen.

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

§ 17 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 Informationssicherheitskonzepten und Betriebskonzepten 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 müssen das Präsidium beziehungsweise der Vorstand in einer Richtlinie regeln.

§ 18 Gefahrenintervention

(1) Um eine gegenwärtige Gefahr für die Informationssicherheit abzuwehren, treffen dezentrales IT-Personal, interne IT-Dienstleister und die 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 Nutzungskonten ergriffen werden. Die jeweils erforderlichen Maßnahmen können auch durch die oder den ISB oder die ISM veranlasst werden sobald sie gegenwärtige Gefahren erkennen.

(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

1.1 In- und Außerkrafttreten

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

(2) Gleichzeitig tritt die Richtlinie zur Informationssicherheit der Georg-August-Universität Göttingen/Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts (Informationssicherheitsrichtlinie - ISRL -) in der Fassung der Bekanntmachung vom 24.01.2020 (AM 04/2020 S. 46 ff.) 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, unerwartetes, unerklärliches oder ungewöhnliches Verhalten von bisher fehlerfrei laufenden Anwendungen, Hardwareausfälle, Eindringen Unbefugter, Manipulationen, Virenbefall u.a.) sind vom jeweiligen IT-Anwender dem zuständigen IT-Personal zwecks Klärung des Problems und ggf. Meldung eines Informationssicherheitsvorfalls an zuständige ISK oder die zuständige Leitung mitzuteilen.

(2) Verhalten von Personen oder Schwachstellen in Prozessen oder IT-Systemen, die die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Prozessen oder IT-Systemen gefährden können, sind dem zuständigen ISK oder der zuständigen Leitung zu melden.

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 werden,

(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 belegen. 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) Aus Anlass der Maßnahme gegebenenfalls zusätzlich erhobene oder über Löschfristen hinaus aufbewahrte 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 oder benutzt 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 oder beim mobilen Arbeiten sind Arbeitsplätze durch ihre Aufstellung oder durch Blickschutzfolien 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 Arbeitsplatzrechner 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.

A.9 Personenbezogene Nutzungskonten

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 Einrichtung von Nutzungskonten, die von mehreren Personen gemeinsam genutzt werden sollen (gemeinsam genutzte Funktionskonten), ist nur zulässig, wenn solche Konten zur Aufgabenerfüllung unverzichtbar sind.

(3) Die Vergabe von Nutzungskonten für die Arbeit an IT-Systemen muss grundsätzlich personenbezogen erfolgen. Die Arbeit unter dem Nutzungskonto einer anderen Person ist unzulässig.

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

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

(6) Der Verzicht auf personenbezogene Nutzungskonten 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) Jede Person ist für alle Handlungen verantwortlich, die unter Verwendung eines ihr zugeordneten Nutzungskontos vorgenommen werden.

(2) Die für Nutzung von IT-Systemen der Stiftungsuniversität Göttingen verwendeten Passwörter (nachfolgend dienstliche Passwörter) dürfen nicht mit Passwörtern

[1] Algorithmus, Schlüssellänge nach Angaben der Bundesnetzagentur

identisch oder ähnlich sein, die zur Nutzung von anderen, nicht der Stiftungsuniversität Göttingen zugeordneten IT-Systemen verwendeten werden. . Die Unterschiede zwischen den Passwörtern müssen signifikant sein, insbesondere dürfen keine systematischen Zusammenhänge bestehen, über die aus einem Passwort das andere erschlossen werden könnte.

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

(a) Passwörter müssen geheim gehalten werden.

(b) Passwörter für persönliche Nutzungskonten dürfen nicht an andere Personen weitergegeben werden.

(c) Für Passwörter von Nutzungskonten, die von mehreren Personen gemeinsam genutzt werden sollen (gemeinsam genutzte Funktionskonten) gilt:

(i) Das Passwort eines Funktionskontos darf nur an die an der Funktion beteiligten Personen weitergegeben werden.

(ii) Beim Ausscheiden einer Person, der das Passwort eines Funktionskontos bekannt ist, muss das Passwort des Funktionskontos geändert werden.

(d) Die Eingabe eines Passwortes muss unbeobachtet stattfinden.

(4) Zur Speicherung von Passwörtern in IT-Systemen gelten folgende Regeln:

(a) Das Abspeichern von dienstlichen Passwörtern in Anwendungen insbesondere Browsern oder auf programmierbaren Funktionstasten ist grundsätzlich nicht zulässig.

(b) Es gelten folgende Ausnahmen von Verbot der Speicherung von dienstlichen Passwörtern:

(i) Die Abspeicherung eines dienstlichen Passworts in der Eduroam-Konfiguration ist auf Desktop- und Laptop-Systemen und auf Smartphones zugelassen.

(ii) Die Abspeicherung von dienstlichen Passwörtern für E-Mail-Zugriffe ist auf einem Smartphone zugelassen.

(iii) Die Abspeicherung von dienstlichen Passwörtern in einem Passwort-Manager mit sicherem Master-Passwort entsprechend der Regelung zur Passwortstärke von Absatz (7) ist zugelassen. Längere Passwörter als Master-Passwort werden empfohlen.

(5) Zum Aufschreiben von Passwörtern auf Papier gelten folgende Regeln

(a) Passwörter auf Papier aufzuschreiben ist zu vermeiden.

(b) Soweit ein Aufschreiben nicht vermeidbar ist, ist das Passwort zumindest so sicher wie eine Scheckkarte oder ein Geldschein aufzubewahren.

(c) Die Hinterlegung eines Passworts in einem verschlossenen Umschlag in einem Tresor, der unter der Aufsicht der Einrichtung steht, für den der Inhaber des Accounts tätig ist, ist zulässig.

(6) Regelungen zur Änderung von Passwörtern:

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

(b) Initial-Passwörter müssen umgehend vor Nutzung der Dienste geändert werden.

(c) Alte Passwörter dürfen nicht wiederverwendet werden

(d) Neue Passwörter und vorhergehend verwendeten Passwörtern müssen sich signifikant unterscheiden, insbesondere dürfen keine systematischen Zusammenhänge bestehen, über die aus dem vorhergehenden Passwort das neue erschlossen werden könnte.

(7) Sofern nicht für bestimmte Passwörter explizit anderer Regeln erlassen wurden, gelten folgende Anforderungen an Passwörter:

(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 mindestens 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.

(8) 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).

(9) 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 Nutzungskonten („Administrator“, „root“ o.a.) vorzunehmen.

(2) Privilegierte Nutzungskonten dürfen nur an IT-Personal vergeben werden bzw. Personen mit privilegierten Nutzungskonten 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, mobiles Arbeiten und Homeoffice

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

(1) Bei Telearbeit, mobilem Arbeiten und im Homeoffice verlassen Daten den räumlich eingegrenzten Bereich der Daten verarbeitenden Stelle.

(2) Zur Einrichtung und zum Betrieb solcher Arbeitsplätze sind die bestehenden Dienstvereinbarungen 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[2] von Daten zu verwenden.

(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 Betriebskonzept 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 Betriebskonzept 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 schützenswerter Daten außerhalb der IT-Systeme der Stiftungsuniversität Göttingen ist nur in den Staaten des europäischen Wirtschaftsraums und sicheren Drittstaaten entsprechend dem Datenschutzrecht zulässig.

[2] Zum Zeitpunkt der Erstellung der Richtlinie z.B. Cryptshare in der UMG.

(6) Die Synchronisation von E-Mails auf privaten Geräten und die damit verbundene Datenspeicherung wird erlaubt, solange nicht zu erwarten ist, dass E-Mails besonders schutzwürdige Inhalte im Sinne von Datenschutz- oder anderen Geheimhaltungsanforderungen enthalten. Für E-Mail-Konten, bei denen aufgrund der Funktion der Kontoinhaber zu erwarten ist, dass E-Mails besonders schutzwürdige Inhalte im Sinne von Datenschutz- oder anderen Geheimhaltungsanforderungen enthalten, ist eine Synchronisation auf private Geräten nicht zulässig.

A.17 Nutzung externer Kommunikationsdienste

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 Betriebskonzepte 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 dienstlichen Daten oder der IT-Infrastruktur der Stiftungsuniversität Göttingen nur erlaubt, wenn die Betriebskonzepte für den jeweiligen Datenbestand und Teilbereich der Infrastruktur oder allgemeine Handlungsanweisungen oder Dienstvereinbarungen dies erlauben.

(2) Ausdrücklich erlaubt ist der Einsatz von privaten Geräten in speziell vorgesehenen Bereichen und dafür vorgesehen Anschlüssen insbesondere in Bibliotheken, an Anschlüssen für Dozenten in Hörsälen und Seminarräumen, in Studierendenarbeitsbereichen oder Gästenetzen 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. Sind personenbezogene Daten vom Verlust betroffen, ist der ISK darauf hinzuweisen, so dass dieser die oder den zuständigen Datenschutzbeauftragten informiert.

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 und vertraulichen Papieren

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

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

(5) 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.

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 in den jeweiligen Betriebskonzepten eindeutig festzulegen.

(2) Konflikte bei Aufgabenzuweisungen und Verantwortungsbereichen sollen durch eine Rollentrennung verhindert werden. Insbesondere bei allen administrativen Anwendungen, die gesetzlichen Anforderungen genügen müssen und Anwendungen, bei denen ein erhöhter Schutzbedarf vorliegt, muss ein Rollenkonzept die Rollentrennung sicherstellen.

(3) 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

(e) Vertretungsregelungen, insbesondere im Administrationsbereich

(f) Zugriffsrechte

(g) Organisation, Verantwortlichkeit und Durchführung der Datensicherung

(h) Installation und Freigabe von Software einschließlich von Softwareaktualisierungen

(i) Zweck, Freigabe und Einsatz selbst erstellter Programme

(j) Dienstanweisungen

(k) Arbeitsanleitungen für Administrationsaufgaben u.ä.

(l) auftretende Informationssicherheits-Ereignisse aller Art

(m) Notfallregelungen

(n) Wartungsvereinbarungen

(o) 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 Nutzungskonten (zum Beispiel root bei UNIX-Systemen). Dort soll der Vertreter nur im Bedarfsfall auf das an geeigneter Stelle hinterlegte Passwort des Nutzungskontos 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[3] beschrieben. Die Zuständigkeit für Brandschutz liegt bei der Feuerwehr und für die weitere Sicherheitsinfrastruktur 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.

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

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 und verpflichtetes 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 angemessen und 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, Betriebskonzepte 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 mit den minimal benötigten Rechten im Betriebssystem 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 Nutzungskonten (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 Nutzungskonto zugeordnet sein. Die Zuordnung von mehreren Nutzungskonten zu einer Person innerhalb eines IT-Systems sollte erfolgen, wenn über die zusätzlichen Konten besondere Rollen abgebildet und besondere Rechte vergeben werden. Auch die zusätzlichen Konten sollten pro Person vergeben werden.

(3) Die Einrichtung von Nutzungskonten, die von mehreren Personen gemeinsam genutzt werden sollen (gemeinsam genutzte Funktionskonten), ist nur zulässig, wenn solche Konten zur Aufgabenerfüllung unverzichtbar sind.

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

(5) 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 Nutzungskonten ohne Administrationsrechte zu verwenden.

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

I.25 Verwaltung von Nutzungskonten 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 Nutzungskonten 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 Nutzungskonto 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 Nutzungskonten 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 Authentifizierungsverfahren zu stellen. Bevorzugt sollte hier eine Mehrfaktor-Authentifizierung erzwungen werden. Sollte diese technisch nicht möglich sein, ist zumindest eine erhöhte Passwortstärke (Komplexität und/oder Länge des Passworts) vorzuschreiben und soweit technisch möglich zu erzwingen.

(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 ihr bzw. 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. Stehen keine anderen Algorithmen zur Begrenzung zur Verfügung, so kann die Begrenzung durch eine Sperrung erfolgen, die entweder nur vom Systemadministrator aufgehoben werden kann oder zeitlich befristet ist.

(e) Es sollen Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen.

(f) 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.

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

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

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

(j) Für Einsatzszenarien mit unterschiedlichen Sicherheitsanforderungen (z.B. Konten für täglicher Arbeiten im Gegensatz zur Konten für Administrationstätigkeiten) sollten unterschiedliche Passwörter oder Authentifizierungsverfahren eingesetzt werden.

(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 (Multi-Faktor-Verfahren) zur Authentifizierung mittels Passwörtern ist soweit technisch umsetzbar einzusetzen, wo über solche Verfahren ein erhöhter Schutzbedarf gewährleistet werden soll oder muss. Für Anwendungen mit normalem Schutzbedarf ist der Einsatz von Multi-Faktoren-Verfahren zu prüfen und nach Möglichkeit einzusetzen.

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 Rollentrennung 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, mobiles Arbeiten und Homeoffice

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 externen Arbeitsplatz 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 externen Arbeitsplatz vertraulich behandelt werden und

(d) das gesamte Verfahren der externen Arbeit revisionssicher ist.

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

(4) Werden bei der externen Arbeit personenbezogene Daten verarbeitet, muss die bzw. der zuständige Datenschutzbeauftragte am Genehmigungsprozess hinzugezogen 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 von den protokollierten Daten mit den Datenschutzbeauftragten, dem Personalrat und der Internen Revision abzustimmen.

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 sowie die Speicherbegrenzung nach Art. 5 Abs. 1 lit. e) 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 höherem 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 Wiedereinspielen von Datensicherungen soll wenigstens einmal jährlich in geeignetem Umfang getestet werden.

I.42 Löschen und Entsorgen von Datenträgern und vertraulichen Unterlagen

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.

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

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

V. Maßnahmen für Verwaltung und Leitung

V.1 Überprüfung bei Personaleinstellung

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	Führungskräfte, Personalabteilung

(1) Qualifikationen und Fähigkeiten sollten vor einer Einstellung geprüft werden

(2) Eine Überprüfung der Angaben dient auch der Prüfung der Vertrauenswürdigkeit.

(3) Für Personal, an das aufgrund der vorgesehenen Tätigkeiten besonderen Anforderungen an die Vertrauenswürdigkeit gestellt werden, sollten zusätzliche Überprüfungen erfolgen (z.B. durch polizeiliche Führungszeugnisse).

V.2 Einweisung bei Einstellung

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	Führungskräfte

(1) Nach der Einstellung ist unverzüglich sicher zu stellen, das neu eingestelltes Personal für die zugewiesenen Aufgaben angemessen in der Informationssicherheitsrichtlinie insbesondere in den relevanten Maßnahmenkatalogen unterwiesen und darauf verpflichtet ist.

(2) Es ist sicher zu stellen, das neu eingestelltes Personal und Personal, bei dem die Aufgabenzuweisung verändert wurde, in die Betriebskonzepte eingewiesen werden, die für die zugewiesenen Aufgaben relevanten sind.

(3) Besondere Berechtigungen sollen nur erteilt werden, wenn eine angemessene Einweisung erfolgt ist und die Befähigung für die zugewiesene Aufgabe sichergestellt wurde.

V.3 Regelmäßige Schulung von Personal

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	Führungskräfte

(1) Grundlegende Schulung zur Informationssicherheit sollen regelmäßig als verpflichtende Präsenzschulung oder Online-Schulung erfolgen.

(2) Schulung für spezifische Informationssysteme sollten entsprechend den Vorgaben der jeweiligen Betriebskonzepte erfolgen.

V.4 Vertretungsregelungen

Verantwortlich für Initiierung:	Zuständige Leitung
Verantwortlich für Umsetzung:	Führungskräfte

(1) Führungskräfte müssen sicherstellen, dass angemessene Vertretungsregelungen für alle Aufgabenbereiche sichergestellt sind.

(2) Vertretungsregelungen sind zu dokumentieren.

Anlage 3 Festlegungen zum Informationssicherheits-Risikomanagement

1 Grundsätze

Diese Anlage ergänzt die Informationssicherheitsrichtlinie um die Festlegungen zum Risikomanagement in der Informationssicherheit.

Das Informationssicherheits-Risikomanagement trägt zum übergreifenden Risikomanagement der Universität bei. Im Informationssicherheits-Risikomanagement ermittelte Risiken fließen entsprechend den Regelungen des übergreifenden Risikomanagements, insbesondere des Risikomanagementkonzepts der Georg-August-Universität (ohne UMG) [1], in dieses ein.

Die in der Informationssicherheitsrichtlinie aufgeführten Grundsätze und Ziele der Informationssicherheit werden hier vorausgesetzt. Um diese Ziele zu erreichen, definiert die Informationssicherheitsrichtlinie einen Informationssicherheitsprozess und legt dazu Grundsätze und Aufgabenverteilungen im Risikomanagement fest. Ziel dieser Anlage ist in Ergänzung zur Informationssicherheitsrichtlinie Methoden für das Risikomanagement und Kriterien für die Risikobewertung festzulegen und die sich daraus und aus der Informationssicherheitsrichtlinie ergebende Aufbau- und Ablauforganisation für das Informationssicherheits-Risikomanagement darzustellen.

Einleitend beschreibt die Anlage die Aufbauorganisation, indem sie die Rollenmodelle der Informationssicherheitsrichtlinie aufgreift und die dort definierten Aufgaben der jeweiligen Rollen im Risikomanagement der Informationssicherheit hervorhebt.

Anschließend definiert die Anlage die zu verwendende Methodik der Risikoanalyse, durch Festlegung der Grundsätze des Informationssicherheits-Risikomanagements, insbesondere der Methoden und Kriterien der Risikoidentifikation, Risikoanalyse, Risikobewertung, Risikobehandlung und Risikoakzeptanz.

Abschließend wird aus Aufbauorganisation und Risiko-Methodik die Ablauforganisation hergeleitet und dargestellt.

Die Anlage orientiert sich an Standards zum Risikomanagement, z.B. ISO/IEC 27005 [2], ONR 49000 bis 49002-2 [3], [4], [5], [6] und dem BSI-Standard 200-3 [7].

Die Anlage berücksichtigt dabei insbesondere die sich aus dem BSI-Gesetz ergebenden Rahmenbedingungen für die von der Universitätsmedizin Göttingen betriebene Kritische Infrastruktur im Gesundheitswesen sowie für die Betrachtung von vernetzten Medizinprodukten zusätzlich den Standard der DIN EN 80001 [8].

2 Aufbauorganisation

Die Aufbauorganisation der Informationssicherheit wird in der Informationssicherheitsrichtlinie beschrieben. Den in der Informationssicherheitsrichtlinie definierten Rollen

sind dort auch Aufgaben für das Informationssicherheits-Risikomanagement zugewiesen. Diese werden hier mit Fokus auf das Informationssicherheits-Risikomanagement ergänzt.

Ergänzt werden die Rollen der Risikobeauftragten für das übergreifende Risikomanagement der Universität gemäß dem Risikomanagementkonzept der Universität [1] aufgeführt.

2.1 Präsidium und Vorstand

Das Präsidium der Universität und der Vorstand der UMG tragen die Gesamtverantwortung für die Informationssicherheit in ihrem jeweiligen Bereich. Diese Gesamtverantwortung schließt die Verantwortung für das Informationssicherheits-Risikomanagement ein. Präsidium und Vorstand obliegt es dabei, die mit dem Informationssicherheits-Risikomanagement verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege zu definieren und aufeinander abzustimmen sowie hierfür angemessene Risikosteuerungs- und Risikocontrolling-Prozesse und diesbezügliche Berichtspflichten zu definieren.

2.2 Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter (ISB)

Die oder der ISB steuert im Auftrag von Präsidium und Vorstand den universitätsweiten Informationssicherheitsprozess der Stiftungsuniversität, darin eingeschlossen auch die Prozesse des Informationssicherheits-Risikomanagements.

Die Rolle schließt die Rolle des Risikomanagers für Informationssicherheit ein.

Die oder der ISB steuert im jährlichen Bericht zur Informationssicherheit an Präsidium und Vorstand einen Bericht zu Informationssicherheitsrisiken bei. Im Bereich der von der UMG betriebenen Kritischen Infrastruktur ist ein zusätzlicher halbjährlicher Bericht der oder des ISB an den Vorstand zu wesentlichen Risiken zu erstellen

2.3 Zuständige Leitung

Die zuständige Leitung ist Risikoeigentümer.

2.4 Fachverantwortliche

Im Rahmen des Informationssicherheits-Risikomanagements unterstützen die Fachverantwortlichen die zuständigen Leitungen bei der Ermittlung aller der Informationswerte als Risikoobjekte. In Betriebskonzepten im Bereich der von der UMG betriebenen Kritischen Infrastruktur sind mindestens jährliche Überprüfungen und ggf. Aktualisierungen durch die Fachverantwortlichen vorzusehen.

2.5 Informationssicherheitskoordinatoren

Im Rahmen des Informationssicherheits-Risikomanagements unterstützen die Informationssicherheitskoordinatoren die zuständigen Leitungen bei der Ermittlung aller der Informationswerte als Risikoobjekte und sind in die Erstellung von Betriebskonzepten eingebunden, indem sie zu den von Fachverantwortlichen erstellten Betriebskonzepten Stellung nehmen.

2.6 Risikobeauftragte

Für die Universität wird im Risikomanagementkonzept [1] die Rolle der Risikobeauftragten definiert. Im Rahmen des Informationssicherheits-Risikomanagements obliegt den Risikobeauftragten die Meldung von Informationssicherheitsrisiken im Rahmen des übergeordneten Risikomanagements. Die dafür nötigen Informationen zu Informationssicherheits-Risiken holen diese dabei bei den zuständigen Leitungen ein (soweit die zuständigen Leitungen nicht gleichzeitig auch Risikobeauftragte sind).

3 Methodik der Risikoanalyse

3.1 Vorbemerkungen

Dieses Kapitel beschreibt die Methodik der Risikoanalyse (Risikomethodik) für das Informationssicherheits-Risikomanagement der Stiftungsuniversität Göttingen.

Risiken werden identifiziert, indem mögliche Gefährdungen und damit verbundene Schadenauswirkungen und Eintrittswahrscheinlichkeiten für Schäden betrachtet werden. Daraus werden Einteilungen in Risikoklassen abgeleitet. Neben der Einteilung in Risikoklassen werden in der Risikomethodik der Stiftungsuniversität Göttingen Klassifizierungen nach Schutzbedarf und Kritikalität betrachtet.

Zur Beurteilung von Schadensauswirkungen werden verschiedene Schadensszenarien für verschiedene Informationssicherheitsziele betrachtet. Grundlage für die Ermittlung von Schadensauswirkungen und Eintrittswahrscheinlichkeiten ist die Betrachtung von Gefährdungen, die sich wiederum aus dem Zusammentreffen von Bedrohungen und Schwachstellen ergeben.

Nachstehend werden die obigen Begriffe erläutert, Zusammenhänge dargestellt. Festlegungen für Klassifikationen werden in der Beschreibung der Ablauforganisation (Kapitel 4) oder in den ergänzenden Informationen (Kapitel 5) getroffen.

3.2 Risikoidentifikation

3.2.1 Schadensszenarien

Für eine systematische Ermittlung von Schadensauswirkungen werden verschiedene Schadensszenarien betrachtet. In Anlehnung an den BSI-Standard 200-1 [9] werden folgende Schadensszenarien im Informationssicherheits-Risikomanagement der Stiftungsuniversität Göttingen betrachtet:

- Beeinträchtigung der Aufgabenerfüllung (sog. Leistungserfüllung entsprechend der ONR 49002-2 [6]),
- Beeinträchtigung der persönlichen Unversehrtheit,
- negative Innen- oder Außenwirkung (sog. Reputation entsprechend der ONR 49002-2 [6]),
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- finanzielle Auswirkungen,
- Verstöße gegen Gesetze, Vorschriften oder Verträge.

Für die Krankenversorgung in der UMG sind Patientensicherheit und Behandlungseffektivität wesentliche Ziele. Die Beeinträchtigung der Erreichung dieser Ziele ist in den Schadenszenarien „Beeinträchtigung der persönlichen Unversehrtheit“ und „Beeinträchtigung der Aufgabenerfüllung“ besonders zu beachten. Die Anforderungen des Standards DIN EN 80001 [8] an Patientensicherheit, Effektivität sowie Daten- und Systemsicherheit werden von den obigen Szenarien, insbesondere „Beeinträchtigung der persönlichen Unversehrtheit“, „Beeinträchtigung der Aufgabenerfüllung“ und „Beeinträchtigung des informationellen Selbstbestimmungsrechts“ ebenso erfasst.

Über das Schadensszenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts“ werden auch die Anforderungen des Datenschutzes in den Informationssicherheits-Risikomanagement-Prozess eingebunden.

3.2.2 Informationssicherheitsziele

Für die systematische Ermittlung von Schadensauswirkungen sind Auswirkungen auf alle Informationssicherheitsziele zu betrachten. Informationssicherheitsziele entsprechend § 3 (1) der Informationssicherheitsrichtlinie sind:

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit.

Für die von der UMG betriebene Kritische Infrastruktur ist entsprechend dem BSI-Gesetz zusätzlich zu betrachten:

- Authentizität, d.h. die Sicherstellung, dass der Informationen von der angegebenen Quelle erstellt wurden.

3.2.3 Schadensauswirkungen

Schadensauswirkungen werden in fünf Kategorien eingeteilt:

- unbedeutend
- gering
- spürbar
- kritisch
- katastrophal

Die Zuordnung zu den die Schadenskategorien erfolgt entsprechend der Tabelle in Abschnitt 5.4 für alle Schadensszenarien aus Abschnitt 3.2.1. Dabei sind jeweils die Auswirkungen von Gefährdungen auf die Erreichung der Informationssicherheitsziele entsprechend Abschnitt 3.2.2 zu betrachten. Die Schadenskategorie ergibt sich dabei aus dem Maximumprinzip, d.h. als Schadenskategorie insgesamt wird die höchsten Schadenskategorie gewertet, die sich bei Betrachtung aller Informationssicherheitsziele und aller Schadenszenarien ergibt.

3.2.4 Eintrittswahrscheinlichkeiten

Um Risiken zu bewerten, sind neben Schadensauswirkungen Eintrittswahrscheinlichkeiten zu betrachten. Soweit eine hinreichend große Datenbasis für die Eintrittswahrscheinlichkeiten vorliegt, ist eine quantitative Bewertung auf Basis von vorhergehenden Ereignissen möglich. Bei fehlender Datenbasis, von der in vielen Fällen auszugehen ist, muss auf eine Schätzung bzw. Einschätzungen zurückgegriffen werden (erfahrungsgeleitete, qualitative Bewertung).

Für die Risikobetrachtung wird eine fünfstufige Kategorisierung von Eintrittswahrscheinlichkeiten vorgenommen. Die Kriterien für eine Zuordnung ergeben sich aus der nachstehenden Tabelle:

Stufe	Interpretation Häufigkeit
Häufig	Einmal pro Monat und häufiger
Möglich	Einmal pro Quartal
Selten	Einmal pro Jahr
sehr selten	Einmal in 3 Jahren
unwahrscheinlich	Seltener als einmal in 3 Jahren

Zur Bestimmung der Eintrittswahrscheinlichkeiten sollen - angelehnt an die Anforderung ANF-RM 23 des B3S [10] - die folgenden Faktoren berücksichtigt werden:

- Schadenshäufigkeit: Sind neue Vorfälle oder Schäden durch Erfahrungswerte zu erwarten?
- Schwachstellenentdeckung: Wie leicht ist die Schwachstelle insbesondere durch potentielle Angreifer zu entdecken?
- Fähigkeit des Angreifers: Welche technischen Fähigkeiten setzt ein erfolgreicher Angriff voraus?
- Exposition der kritischen Komponente: In welchem Maß ist das System durch seine räumliche Lage einer potenziellen Bedrohung durch ein natürliches Ereignis ausgesetzt?
- Güte der Maßnahmen zur Angriffsentdeckung: Wie schnell kann ein tatsächlich stattfindender Angriff durch die Angegriffenen entdeckt werden?

3.2.5 Bedrohungen, Schwachstellen und Gefährdungen

Grundsätzlich ergeben sich Gefährdungen aus dem Zusammentreffen von Bedrohungen und Schwachstellen. Dabei geht diese Richtlinie bei der Identifikation von Gefährdungen und Bedrohungen von einem All-Gefahrenansatz aus.

Für die Risikoanalyse greift die Stiftungsuniversität Göttingen im ersten Schritt auf vorgefertigte Gefährdungskataloge zurück. Als Basis für eine Gefährdungsidentifikation wird der Katalog der elementaren Gefährdungen des Bundesamts für Sicherheit in der Informationsverarbeitung (BSI) im BSI-Standard 200-3 (s. Abschnitt 5.3.1) herangezogen. Für die Krankenversorgung wird zusätzlich auf den Branchenspezifischen Sicherheitsstandard (B3S) und darin enthaltene spezifische Gefahren zurückgegriffen (s. Abschnitt 5.3.2).

Eine explizite Betrachtung von Bedrohungen und Schwachstellen und darauf basierend die Ableitung von weiteren Gefährdungen muss erfolgen, wenn die vorliegenden Gefährdungskataloge unzureichend erscheinen.

Zur Orientierung bei der Ermittlung von Bedrohungen steht in Abschnitt 5.1 eine Liste möglicher Bedrohungen bereit.

Erst durch Ausnutzung von Schwachstellen ergeben sich aus potentiellen Bedrohungen reale Gefährdungen und daraus abgeleitet Risiken. Die Betrachtung von Schwachstellen ist daher zur Identifikation von Gefährdungen wesentlich, da sich aus einer Bedrohung nur dann eine Gefährdung ergeben kann, wenn diese mit einer Schwachstelle zusammentrifft. Für die Betrachtung von Schwachstellen ist in Abschnitt 5.2 eine Liste möglicher Schwachstellen aufgeführt.

Beide Listen sollen für weitergehende Analysen herangezogen werden, wenn Lücken in den Gefährdungskatalogen identifiziert wurden.

3.3 Risikobewertung

3.3.1 Schutzbedarf

Die Risikomethodik der Stiftungsuniversität Göttingen sieht in Anlehnung an den BSI-Standard 200-1 [9] als ersten Schritt der Risikoanalyse eine Schutzbedarfsfeststellung vor.

Der Schutzbedarf für einen Informationswert betrachtet mögliche Schadensauswirkungen durch potentiell einwirkende Gefährdungen, ohne Eintrittswahrscheinlichkeiten zu berücksichtigen, und vor einer möglichen Risikoreduktion durch Informationssicherheitsmaßnahmen.

Die Informationssicherheitsrichtlinie legt in § 4 (2) drei Schutzbedarfskategorien fest

Für die Zuordnung von Schadensauswirkungen zu den Schutzbedarfskategorien wird

auf die Kriterien zur Klassifikation von Schadensauswirkungen nach Abschnitt 5.4 zurückgegriffen. Dabei werden die Schadenskategorien wie folgt den Schutzbedarfskategorien zugeordnet:

- Normaler Schutzbedarf ergibt sich für die Schadenskategorie unbedeutend,
- hoher Schutzbedarf für die Schadenskategorien gering und spürbar,
- sehr hoher Schutzbedarf für die Schadenskategorien kritisch und katastrophal.

Für Informationswerte, für die ein normaler Schutzbedarf festgestellt wird, kann eine umfassende Risikoanalyse entfallen. Für diese Informationswerte müssen die Maßnahmen des Maßnahmenkatalogs für den IT-Grundschutz entsprechend Anlage 2 der Informationssicherheitsrichtlinie umgesetzt werden.

Hoher oder sehr hoher Schutzbedarf ergibt sich auch zwingend aus der Datenschutzgesetzgebung bei der Bearbeitung besonderer Kategorien personenbezogener Daten, also insbesondere auch immer bei der Bearbeitung von Gesundheitsdaten im Rahmen der Krankenversorgung.

3.3.2 Kritikalität

Für Informationswerte und IT-Systeme im Bereich der von der UMG betriebenen Kritischen Infrastruktur gemäß BSI-Gesetz ist die Kritikalität von IT-Systemen zu bewerten, die sich aus den Verfügbarkeitsanforderungen der Informationswerte und IT-Systeme ergibt. Die Klassifizierung orientiert sich am Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus [10], der drei Kritikalitätsklassen 1 bis 3 vorsieht, je nachdem, ob ein Ausfall von Systemen für eine kurze, mittlere oder längere Dauer kompensiert werden kann.

Die Festlegung der Kritikalität dient dabei der Priorisierung der Risikoanalysen und Risikobehandlung oder der Prüfungen.

Für die Stiftungsuniversität Göttingen wird die Zuordnung dabei wie folgt festgelegt:

- Klasse 1: Systeme, deren Ausfall für höchstens 2 Stunden kompensiert werden kann.
- Klasse 2: Systeme, deren Ausfall für mehr als zwei Stunden, aber höchstens 1 Tag kompensiert werden kann.
- Klasse 3: Systeme, deren Ausfall für mehr als einen Tag kompensiert werden kann.

3.3.3 Risikoklassen

In einer Risikomatrix werden Schadensauswirkung gegen Eintrittswahrscheinlichkeit aufgetragen und Paaren dieser Werte darin den Risikoklassen zugeordnet.

Für die Stiftungsuniversität Göttingen werden folgende Risikoklassen festgelegt:

- vertretbare Risiken

  Risiken, die als hinreichend gering angesehen werden, so dass diese ohne weitere Maßnahmen, z.B. zur Risikoreduktion, akzeptiert werden können.

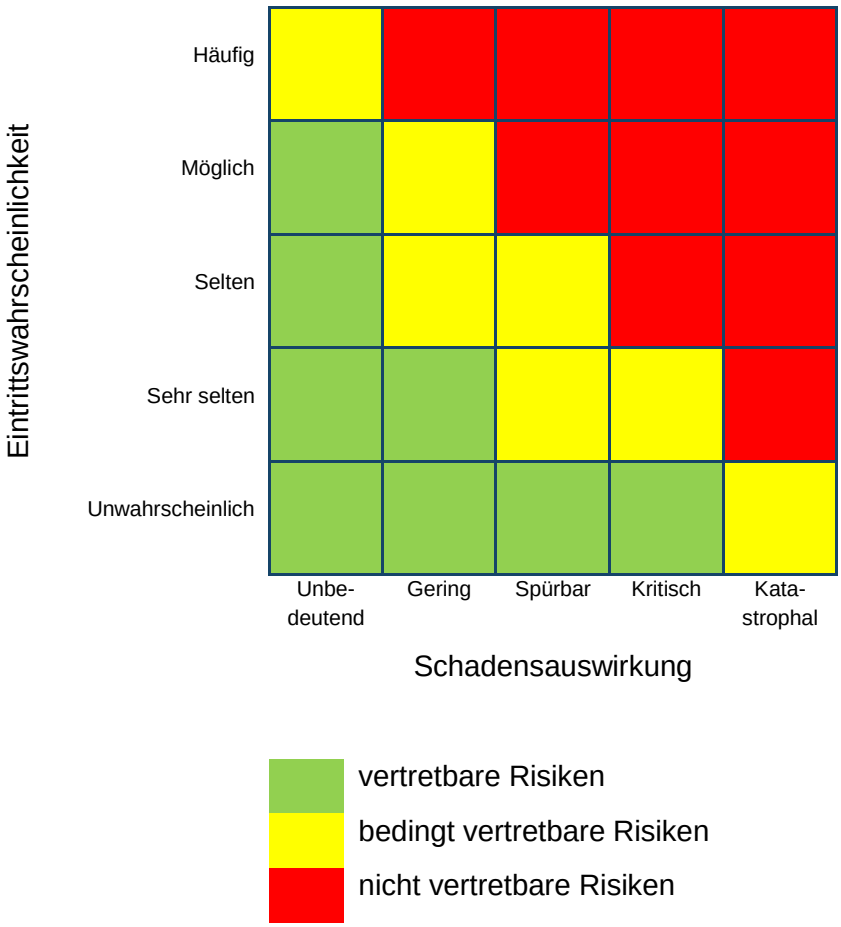
- bedingt vertretbare Risiken

  Risiken, die nach Möglichkeit weiter reduziert werden sollten (in den Bereich geringer Risiken), aber mit Begründung, warum eine weitergehende Risikobehandlung nicht möglich oder sinnvoll ist, von der zuständigen Leitung akzeptiert werden können. Die Risikoakzeptanz und die Begründung hierfür müssen dokumentiert werden.

- nicht vertretbare Risiken

  Risiken, die grundsätzlich nicht akzeptiert werden können. Ausnahmen in besonderen und ausdrücklich mit Hinweis auf die eigentlich vorhandene Grenzüberschreitung begründeten Fällen können nur von Präsidium oder Vorstand beschlossen werden.

Die Zuordnung der Risikoklassen erfolgt entsprechend der nachstehenden Risikomatrix:



3.4 Risikobehandlung

An Risikoidentifikation und Risikobewertung muss eine Risikobehandlung angeschlossen werden. Für die Behandlung von Risiken sind grundsätzlich folgende Verfahren möglich:

- **Risikovermeidung**: Risikovermeidung bedeutet, dass Risikoursachen ausgeschlossen werden, z.B. auch durch Verzicht auf den Einsatz bestimmter Prozesse oder Systeme.
- **Risikoreduktion**: Risikoreduktion bedeutet, dass Risiken durch geeignete Maßnahmen, die Schadensauswirkungen oder Eintrittswahrscheinlichkeiten eines Schadens verringern, reduziert werden.
- **Risikotransfer**: Risikotransfer bedeutet, dass Risiken mit einer anderen Partei geteilt werden, z.B. durch Abschluss von Versicherungen oder durch Outsourcing.
- **Risikoakzeptanz**: Risikoakzeptanz bedeutet, dass Risiken bewusst getragen werden, weil z.B. die durch eine Aktivität gegebenen Chancen wahrgenommen werden sollen, und andere Risikobehandlungen nicht oder nicht sinnvoll angewandt werden können oder die Risiken unterhalb der Risikoakzeptanzschwelle liegen.

Risikotransfer ist im Bereich der Kritischen Infrastrukturen generell und somit auch für die von der UMG betriebene Kritische Infrastruktur nur bedingt, d.h. zur Absicherung von Restrisiken, anwendbar (s. [11] und ANF-RM 27 in [10]).

4 Ablauforganisation

4.1 Ermittlung der Informationswerte (Risikoobjekte) und Risikoeigentümer

Die Stiftungsuniversität Göttingen ist in Lehre, Forschung und Krankenversorgung tätig. Die Prozesse, die diese Tätigkeitsbereiche ermöglichen, und alle Informationen, die zur Aufrechterhaltung der Prozesse dienen, stellen die primären Werte der Stiftungsuniversität Göttingen dar. Die primären Werte sind abhängig von unterstützenden Prozessen und IT-Systemen (sekundären Werten). Die Dezentralität und Heterogenität von Lehre, Forschung und (teilweise) Krankenversorgung erfordert eine Identifikation der Werte in dezentralen Einheiten der Stiftungsuniversität Göttingen.

Die Verantwortung für die Ermittlung von Informationswerten als Risikoobjekte in ihrem Zuständigkeitsbereich obliegt den zuständigen Leitungen als Risikoeigentümer für diese Risikoobjekte. Die Fachverantwortlichen und Informationssicherheitskoordinatoren unterstützen die zuständigen Leitungen bei der Ermittlung von Informationswerten und den weiteren Schritten der Risikoanalyse.

4.2 Feststellung des Schutzbedarfs und der Kritikalität

Die Fachverantwortlichen ermitteln im Rahmen der Erstellung von Betriebskonzepten den Schutzbedarf für Informationswerte unter Betrachtung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und soweit nötig (z.B. bei Betrachtung der von der UMG betriebenen Kritischen Infrastruktur) Authentizität.

Der Schutzbedarf ergibt sich aus der Betrachtung der Schadensszenarien entsprechend Abschnitt 3.2.1 und der Klassifikation der Schadensauswirkungen entsprechend Abschnitt 3.2.3. Grundlage hierfür ist die Betrachtung von Gefährdungen entsprechend Abschnitt 3.2.5.

Eine Betrachtung von Eintrittswahrscheinlichkeiten und somit die Ermittlung von Risiken erfolgt bei der Feststellung des Schutzbedarfs noch nicht.

Die Kritikalität entsprechend Abschnitt 3.3.2 ist zusätzlich für die von der UMG betriebene Kritische Infrastruktur im Gesundheitswesen zu betrachten.

Ergebnisse der Feststellung des Schutzbedarfs und der Kritikalität sind als Teil der Betriebskonzepte zu dokumentieren.

4.3 Risikoanalyse

Für Informationswerte mit einem normalen Schutzbedarf wird davon ausgegangen, dass mit der Umsetzung von Maßnahmen des IT-Grundschutzes entsprechend der Informationssicherheitsrichtlinie ein ausreichendes Informationssicherheitsniveau erreicht wird.

Für Informationswerte mit einem höheren Schutzbedarf muss im Rahmen der Erstellung von Betriebskonzepten eine Risikoanalyse durchgeführt und dokumentiert werden. Für alle Informationswerte in der Krankenversorgung ist von einem höheren Schutzbedarf auszugehen, so dass für diesen Bereich eine Risikoanalyse erfolgen muss.

Für die Risikoanalyse sind die Schritte Risikoidentifikation (s. Abschnitt 3.2), Risikobewertung (s. Abschnitt 3.3) und Risikobehandlung (s. Abschnitt 3.4) von den zuständigen Fachverantwortlichen durchzuführen. Die Risikobehandlung ist von den Fachverantwortlichen und dem zuständigen IT-Personal umzusetzen und zu dokumentieren, wobei dem Fachverantwortlichen die Kontrolle obliegt.

Aus den so ermittelten Schadensauswirkungen und Eintrittswahrscheinlichkeiten ergibt sich entsprechend Abschnitt 3.3.3 das Risiko als Zuordnung zu einer Risikoklasse.

Wird im Risikobehandlungsplan das Verfahren der Risikoreduktion eingesetzt, so muss auf Basis bereits umgesetzter oder konkret geplanter Maßnahmen eine erneute Risikoidentifikation im Hinblick auf Reduktion von Schadensauswirkungen und Eintrittswahrscheinlichkeiten und darauf basierend eine Risikobewertung durchgeführt wer-

den. Die Reduktionseffekte sind bzgl. Schadensauswirkung und Eintrittswahrscheinlichkeit sowie der sich daraus ergebenden Zuordnung zu einer Risikoklasse zu dokumentieren.

Nach Umsetzung der Risikobehandlung ist die Risikoanalyse solange zu wiederholen, bis die verbleibenden Risiken vollständig behandelt wurden, d.h. alle verbliebenen Risiken akzeptiert wurden.

4.4 Überwachung

4.4.1 Überwachung der Umsetzung

Bei der Überwachung der Umsetzung der im Rahmen von Risikobehandlungsplänen festgelegten Maßnahmen zur Risikoreduktion durch Fachverantwortliche und übergeordnet durch die zuständigen ISM sind neben der Konformität zum Behandlungsplan auch die Wirksamkeit und Angemessenheit der Maßnahmen zu prüfen.

Die Ergebnisse der Prüfung sind als Anlagen der Betriebskonzepte zu dokumentieren.

4.4.2 Überwachung von Richtlinien und Konzepten

Die Informationssicherheitsrichtlinie, die übergreifenden Informationssicherheitskonzepte und Betriebskonzepte sind regelmäßig zu überprüfen und zu aktualisieren. Dabei sind alle Veränderungen an Informationswerten, Bedrohungen, Schwachstellen, Schadensauswirkungen, Eintrittswahrscheinlichkeiten, Risiken und Risikobehandlungsoptionen zu betrachten.

Die Informationssicherheitsrichtlinie und übergreifende Informationssicherheitskonzepte sind jährlich zu überprüfen. Die Prüfung erfolgt durch den Informationssicherheitsbeauftragten in Zusammenarbeit mit dem Datenschutz- und Informationssicherheits-Beirat. Die Ergebnisse der Prüfung sind dem Präsidium und dem Vorstand als Bericht vorzulegen. Präsidium und Vorstand beschließen auf Basis des Berichts über Beibehaltung oder Änderungen an der Informationssicherheitsrichtlinie und der übergreifenden Informationssicherheitskonzepte.

Betriebskonzepte einschließlich der Risikoanalyse und der Risikobehandlung werden entsprechend der in diesen Konzepten festgelegten Intervallen durch die Fachverantwortlichen überprüft und bei Bedarf überarbeitet. Die auf Basis von Prüfergebnissen und überarbeiten Betriebskonzepte werden der zuständigen Leitung zum Beschluss und der oder dem Informationssicherheitsbeauftragten zur Zustimmung vorgelegt.

4.5 Kommunikation und Konsultation

Die Unterrichtung von Präsidium und Vorstand über Risiken erfolgt im Rahmen des jährlichen Berichts der oder des ISB gemäß § 11 Abs. (2) Buchst. (g).

Der Bericht nach § 11 Abs. (2) Buchst. (g) führt die übernommenen Informationssicherheitsrisiken auf. Der Schwerpunkt liegt dabei auf Risiken, die gemäß dieser Anlage der

Risikoklassen „bedingt vertretbar“ und „nicht vertretbar“ zuzuordnen sind. Die Veränderung der Risikosituation und die Ergebnisse der Überwachung der Risiken, die Maßnahmenverfolgung hinsichtlich Wirksamkeit der Maßnahmen sowie Entscheidungsbedarfe sind im Bericht aufzuführen.

Basis des Berichts sind die von den zuständigen Leitungen beschlossenen Betriebskonzepte und die Fortschreibungsergebnisse derselben.

Im Bereich der von der UMG betriebenen Kritischen Infrastruktur ist ein zusätzlicher halbjährlicher Bericht der oder des ISB an den Vorstand zu wesentlichen Risiken zu erstellen.

Im Bereich der Universität (ohne UMG) erfolgt ein übergreifendes Risikomanagement, das im Risikomanagement-Konzept der Universität beschrieben ist. Überschreiten Informationssicherheitsrisiken im Bereich der Universität die in diesem Risikomanagement-Konzept festgelegten Schwellenwerte zur Erfassung von Risiken, werden diese Risiken durch die entsprechend diesem Risikomanagement-Konzept zuständigen Risikobeauftragten zur Aufnahme in den Risikobericht gemeldet.

5 Ergänzende Informationen

5.1 Liste Bedrohungen

Die nachstehende Liste von Bedrohungen ist dem Leitfaden „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“ [12] des BSI bzw. der dazugehörigen Anlage „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Hilfsmittel“ [13] entnommen. Die Nummerierung wurde ergänzt. Die Bedrohungen B 4.2.6, B 4.3.1 und B 4.4.1 wurden in Anlehnung an die Bedrohungen A1.4, A1.11 und A1.10 der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG Version 1.0“ [14] des BSI ergänzt.

B 1 Natürliche Ereignisse
B 1.1 Natürliche Ereignisse (Blitz, Feuer, Wasser, Staub, Klima, Wind)
B 2 Technisches Versagen
B 2.1 Technisches Versagen von IT-Systemen
B 2.1.1 Fehlfunktion von IT-Systemen
B 2.1.2 Störung oder Ausfall von IT-Systemen
B 2.2 Technisches Versagen von Datenspeichern
B 2.2.1 Verschleiß von Speichermedien
B 2.2.2 Datenverlust
B 2.3 Technisches Versagen von Netzen
B 2.3.1 Störung oder Ausfall von Kommunikationsnetzen
B 2.4 Technisches Versagen der Versorgung
B 2.4.1 Störung oder Ausfall der Stromversorgung
B 2.4.2 Störung oder Ausfall von Versorgungsnetzen
B 3 Menschliche Fehlhandlungen
B 3.1 Menschliche Fehlhandlungen an IT-Systemen
B 3.1.1 Fehlerhafte Nutzung oder Administration von IT-Systemen

B 3.2 Menschliche Fehlhandlungen an Software
B 3.2.1 Software-Schwachstellen oder –Fehler
B 3.3 Menschliche Fehlhandlungen mit Daten
B 3.3.1 Unbeabsichtigte Offenlegung schützenswerter Informationen
B 4 Vorsätzliche Handlungen
B 4.1 Vorsätzliche Handlungen an IT-Systemen
B 4.1.1 Manipulation von Hardware
B 4.1.2 Diebstahl und Verlust von Systemen, Datenträgern und Dokumenten
B 4.1.3 Unbefugtes Eindringen in Räumlichkeiten
B 4.1.4 Unbefugtes Eindringen in IT-Systeme
B 4.1.5 Unberechtigte Nutzung oder Administration von IT-Systemen
B 4.1.6 Zerstörung von IT-Systemen
B 4.2 Vorsätzliche Handlungen an Software, Daten und Informationen
B 4.2.1 Abstreiten von Handlungen
B 4.2.2 Ausspähen von Informationen / Daten
B 4.2.3 Manipulation von Software und Informationen / Daten
B 4.2.4 Missbrauch personenbezogener Daten (z.B. schützenswerter Personen)
B 4.2.5 Missbrauch von Berechtigungen
B 4.2.6 Identitätsmissbrauch
B 4.2.7 Zerstörung von Datenträgern
B 4.3 Vorsätzliche Handlungen an Datennetzen
B 4.3.1 (Distributed) Denial-of-Service-Angriffe (DoS, DDoS)
B 4.4 Vorsätzliche Handlungen in zwischenmenschlicher Kommunikation
B 4.4.1 Social Engineering
B 5 Organisatorische Einflüsse
B 5.1 Interne organisatorische Einflüsse
B 5.1.1 Ressourcenmangel (Fehlplanung)
B 5.2 Externe organisatorische Einflüsse
B 5.2.1 Störung oder Ausfall von Dienstleistern

Bei der Betrachtung menschlicher Fehlhandlung und vorsätzlicher Handlungen sind Innen- und Außentäter zu berücksichtigen, weiter sind Personen mit physischem Zugang wie auch mit nur einem Netzzugang zu bedenken.

5.2 Liste Schwachstellen

Die nachstehende Liste von Schwachstellen ist dem Leitfaden „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“ [12] des BSI bzw. der dazugehörigen Anlage „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Hilfsmittel“ [13] entnommen. Die Nummerierung wurde ergänzt. S 3.4.5 wurde in Anlehnung an Schwachstelle A 2.7 der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG Version 1.0“ [14] ergänzt.

S 1 Hardware
S 1.1 Unsachgemäße Entsorgung
S 1.2 Unzureichende Umgebungsbedingungen

S 1.2.1 Das System ist nicht resistent gegen Feuchtigkeit, Staub oder Verunreinigung
S 1.2.2 Das System ist nicht resistent gegen Hitze oder Kälte
S 1.2.3 Das System ist an ungeeignetem Standort platziert
S 1.3 Unzureichende Instandhaltung
S 1.4 Unsichere und/oder nicht nachvollziehbare Hardwarekonfiguration
S 1.4.1 Unvollständige und/oder fehlerhafte Dokumentation der Hardwarekonfiguration
S 1.4.2 Änderungen an der Hardware werden nicht ausreichend dokumentiert
S 1.4.3 Änderungen an der Hardware werden nicht überwacht

S 2 Software

S 2.1 Mangelnder Malwareschutz
S 2.2 Bekannte Softwarefehler
S 2.3 Mangelnde Sicherheitsfunktionalität
S 2.3.1 Unzureichender Passwortschutz
S 2.3.2 Unzureichende Verschlüsselung
S 2.3.3 Mangelnder Zugriffsschutz
S 2.4 Unsichere Softwarekonfiguration
S 2.4.1 Mangelndes Patch-Management
S 2.4.2 Unzureichende Standardkonfiguration

S 3 Netz

S 3.1 Fehlende Verschlüsselung
S 3.1.1 Ungeschützte Verbindungen in öffentliche Netze (insb. ungeschützte WLAN-Zugänge)
S 3.1.2 Ungeschützte Kommunikationsverbindungen
S 3.1.3 Übertragung von Kennworten in Klartext
S 3.2 Physikalische Mängel
S 3.2.1 Mangelhafte Verkabelung
S 3.2.2 Ungeschützte Netzwerkanschlüsse
S 3.3 Unsachgemäßes Netzwerkmanagement
S 3.3.1 Routing Widerstandsfähigkeit gegen Störungen
S 3.3.2 Mangelhaftes Netzwerkkonfigurationsmanagement
S 3.4 Unsichere Netzwerkarchitektur
S 3.4.1 Single point of failure
S 3.4.2 Unbekannte IT-Systeme
S 3.4.3 Bekannte kompromittierte IT-Systeme
S 3.4.4 Mangelnde Mechanismen für Identifikation und Authentisierung
S 3.4.5 Verkopplung von Diensten und mangelnde Trennung zur Störungsvermeidung und Störungsisolation

S 4 Personal

S 4.1 Nicht ausreichende Besetzung kritischer Personalressourcen
S 4.2 Unzureichende Anwenderschulung
S 4.3 Mangelnde Sorgfalt bei der Personalauswahl

S 5 Infrastruktur

S 5.1 IT-Systeme sind frei zugänglich
S 5.2 Mangelnde Gebäudesicherheit
S 5.2.1 Mangelnder Zutrittsschutz
S 5.2.2 Mangelnder Schutz vor Wasserschäden

S 5.2.3 Mangelnder Brandschutz
S 5.2.4 Ungünstiger Gebäudestandort
S 5.3 Unzureichend sichere Stromversorgung
S 5.3.1 Spannungs- und Frequenzschwankungen
S 5.3.2 Abhängigkeit von einem einzigen Energieversorger
S 5.3.3 Fehlende Notstromkapazität
S 6 Organisation
S 6.1 Unzureichende Prozesse
S 6.1.1 Mangelndes Dienstleister-Management
S 6.1.2 Unzureichende Prozesse für Security- und Risiko-Management
S 6.1.3 unregelmäßige Backups
S 6.1.4 Mangelndes Endgerätemanagement
S 6.1.5 Unzureichende Notfallplanung
S 6.1.6 Mangelndes Logging und Monitoring
S 6.1.7 Mangelndes Hardware und Software Konfigurationsmanagement
S 6.1.8 Keine durchgängige Verwaltung von Hardware- oder Softwarebeständen
S 6.2 Unzureichende Verantwortlichkeiten
S 6.2.1 Es gibt keinen Verantwortlichen
S 6.2.2 Es gibt keinen eindeutig benannten Verantwortlichen
S 6.3 Unzureichende Rollendefinition
S 6.3.1 Unvollständige Aufgabenbeschreibung von Rollen
S 6.3.2 Mangelndes Identitäts- und Berechtigungsmanagement (Identity and Access Management, IAM)

5.3 Listen von Gefährdungen

5.3.1 Elementare Gefährdungen des BSI-Grundschutzes

Die nachstehende Liste elementarer Gefährdungen ist dem BSI-Standard 200-3 entnommen. In der Spalte Grundwert ist vermerkt, welche Grundwert/Informationssicherheitsziele von der Gefährdung betroffen sein können (C=Confidentiality/Vertraulichkeit, I=Integrity/Integrität, A=Availability/Verfügbarkeit)

Nummer	Gefährdung	Grundwert
G 0.1	Feuer	A
G 0.2	Ungünstige klimatische Bedingungen	I, A
G 0.3	Wasser	I, A
G 0.4	Verschmutzung, Staub, Korrosion	I, A
G 0.5	Naturkatastrophen	A
G 0.6	Katastrophen im Umfeld	A
G 0.7	Großereignisse im Umfeld	C, I, A
G 0.8	Ausfall oder Störung der Stromversorgung	I, A
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A
G 0.12	Elektromagnetische Störstrahlung	I, A
G 0.13	Abfangen kompromittierender Strahlung	C
G 0.14	Ausspähen von Informationen/Spionage	C
G 0.15	Abhören	C

G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C, A
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	C, A
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen aus unzuverlässiger Quelle	C, I, A
G 0.21	Manipulation von Hard- und Software	C, I, A
G 0.22	Manipulation von Informationen	I
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I
G 0.24	Zerstörung von Geräten oder Datenträgern	A
G 0.25	Ausfall von Geräten oder Systemen	A
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A
G 0.27	Ressourcenmangel	A
G 0.28	Softwareschwachstellen oder –fehler	C, I, A
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.32	Missbrauch von Berechtigungen	C, I, A
G 0.33	Personalausfall	A
G 0.34	Anschlag	C, I, A
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A
G 0.36	Identitätsdiebstahl	C, I, A
G 0.37	Abstreiten von Handlungen	C, I
G 0.38	Missbrauch personenbezogener Daten	C
G 0.39	Schadprogramme	C, I, A
G 0.40	Verhinderung von Diensten (Denial of Service)	A
G 0.41	Sabotage	A
G 0.42	Social Engineering	C, I
G 0.43	Einspielen von Nachrichten	C, I
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A
G 0.45	Datenverlust	A
G 0.46	Integritätsverlust schützenswerter Informationen	I
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	C, I, A

5.3.2 Gefährdungen des B3S

Die nachstehenden Gefährdungen sind dem Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus der DKG [10] entnommen. Diese Gefährdungen sind für Informationswerte in der von der UMG betrieben Kritischen Infrastruktur im Gesundheitswesen zusätzlich zu betrachten.

GEF 1 Nichtverfügbarkeit wichtiger, medizinisch relevanter Daten im Diagnose-Prozess

GEF 2 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Therapie-Prozess

GEF 3 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Pflege-Versorgungs-Prozess
GEF 4 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Entlassungs-Prozess
GEF 5 Nichtverfügbarkeit von für den Behandlungsprozess wichtiger Prozess- und Freigabeinformationen
GEF 6 Nichtverfügbarkeit von behandlungsprozessrelevanten IT-Systemen
GEF 7 Nichtverfügbarkeit von behandlungsrelevanten Logistikketten
GEF 8 Inkonsistenzen in für den Behandlungsprozess relevanten Datenbeständen
GEF 9 Inkonsistenzen bei der Übertragung von für den Behandlungsprozess relevanten Datenbeständen
GEF 10 Manipulation von medizinisch relevanten Daten im Diagnose-Prozess
GEF 11 Manipulation von medizinisch relevanten Daten im Therapie-Prozess
GEF 12 Manipulation von medizinisch relevanten Daten im Versorgungs-Pflege-Prozess
GEF 13 Manipulation von medizinisch relevanten Daten im Entlassungs-Prozess
GEF 14 Unterbrechung von behandlungsrelevanten Kommunikationsabläufen.
GEF 15 Vertraulichkeitsverlust bei besonders sensiblen Patienten- und Behandlungsinformationen.
GEF 16 Verlust der Datenauthentizität
GEF 17 Fremdsteuerung/Manipulation von medizinische relevanten IT-Systemen
GEF 18 Fremdsteuerung/Manipulation von netzangebundenen Medizingeräten
GEF 19 Fremdsteuerung/Manipulation von relevanten Infrastrukturkomponenten

5.4 Kriterien für die Zuordnung zu Schadensauswirkungskategorien und Schutzbedarf

Die Zuordnung zu den fünf Kategorien von erfolgt entsprechend den Kriterien der nachstehenden Tabelle:

Stufe	Persönliche Unversehrtheit	Aufgabenerfüllung	Negative Innen- oder Außenwirkung	Finanzielle Auswirkungen	Informationelles Selbstbestimmungsrecht	Verstoß gegen Gesetze, Verordnung, Vorschriften, Verträge	Schutz-bedarf
Unbedeutend	Vorkommnis, jedoch ohne Folgen (critical incident, near miss).	bleibt unberührt.	Die Reputation wird kaum beeinträchtigt. Es entsteht intern Klärungsbedarf.	Der finanzielle Schaden ist im Jahresergebnis kaum wahrnehmbar.(Universität bis 100.000 €, UMG bis 200.000€).	Unberechtigter Zugriff auf Daten, die an anderen Stellen von den Betroffenen frei zugänglich gemacht wurden.	Ohne Verstöße gegen Vorschriften und Gesetze, keine, oder nur geringfügige Schadensersatzforderungen	normal
gering	Leichter Gesundheitsschaden mit vorübergehenden Beschwerden/Schmerzen bis zu 3 Tagen Hospitalisation oder im Falle von Patienten der UMG verlängerte Hospitalisation.	bleibt unberührt, es entstehen kurzzeitige Störungen im Betriebsablauf und Mehrkosten.	Nachfragen von interessierten Personen außerhalb der Universität, die Medien interessieren sich. Der externe Klärungsbedarf hat noch keine anhaltenden Folgen.	Der finanzielle Schaden führt zu geringen Abweichungen im Jahresergebnis (Universität bis 300.000 €, UMG bis 500.000 €).	Unberechtigter Zugriff auf Daten, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen, geringfügige Schadensersatzforderungen bis 300.000 €; Bußgelder bis 10.000 €	hoch
spürbar	Schwerer Gesundheitsschaden ohne Dauerfolgen. Mehr als 3 Tage (verlängerte) Hospitalisation.	Vorübergehend vermindert. Es entstehen Mehrkosten aus der Behandlung und/oder aus zusätzlichen Störungen der Prozesse.	Die Reputation wird durch negative Berichte, Untersuchung und lokale Medienberichte beeinträchtigt.	Der finanzielle Schaden hat negative Auswirkungen auf das Jahresergebnis. Sowohl der Ertrag als auch die Liquidität werden sichtlich beeinträchtigt (Universität bis 1.000.000 €, UMG bis 3.000.000 €).	Unberechtigter Zugriff auf Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen").	Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen, über 1.000.000 €; Bußgelder bis 100.000 €; Strafbarkeit	
kritisch	Schwerer Gesundheitsschaden mit Dauerfolgen, ohne dauerhafte Pflegebedürftigkeit, jedoch mit Berufseinschränkung.	andauernd beeinträchtigt. Das Leistungsangebot wird eingeschränkt.	Die Reputation wird regional über längere Zeit geschädigt, durch negative Medienberichte, Straf- und Haftpflichtklagen und Untersuchungen. Studierende, Forschungspartner oder Patienten bevorzugen nach Möglichkeit andere Universitäten oder Kliniken.	Das finanzielle Ergebnis wird nachhaltig beeinflusst. Der Schaden steigt auf die Höhe eines Jahresergebnisses. Die Liquidität wird angespannt (Universität bis 3.000.000 €, UMG bis 5.000.000 €).	Unberechtigter Zugriff auf Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz").	Schwere Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen, Schadensersatzforderungen über 1.000.000 €; Bußgelder über 100.000 €; erhebliche Strafbarkeit	Sehr hoch
katastrophal	Schwerer Gesundheitsschaden mit Dauerfolgen und dauerhafter Pflegebedürftigkeit. Todesfall.	Die Fortführung einer Einrichtung (Institut, Klinik, Abteilung, Bereich) mit bisherigem Leistungsspektrum ist bedroht.	Die Reputation wird überregional, irreparabel geschädigt, z. B. durch Strafrechtsklagen und negative Berichtserstattung. Das Vertrauen in die Führung ist erschüttert, die Kapazitätsauslastung ist dadurch nicht mehr sichergestellt.	Der finanzielle Schaden ist existenzgefährdend und hat schwere Auswirkungen auf das Jahresergebnis. Es droht die Zahlungsunfähigkeit (Universität über 3.000.000 €, UMG über 5.000.000 €)	Unberechtigter Zugriff auf Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Fundamentaler Verstoß gegen Vorschriften und Gesetze, Schadensersatzforderungen über 3.000.000 €; Bußgelder über 1.000.000 €; Strafbarkeit bis hin zu Verbrechen	

Abschnitt V: Literaturverzeichnis

[1] Georg-August-Universität Göttingen, „Risikomanagementkonzept der Georg-August-Universität Göttingen," https://www.uni-goettingen.de/de/document/download/c4666b41203f78adb6d0a510c4908639.pdf/Risikomanagement_Konzept.pdf, 2020.

[2] ISO/IEC, „ISO/IEC 27005:2011(E): Information technology — Security techniques — Information security risk management," ISO/IEC, Genf, 2011.

[3] Austrian Standards Institute, „ONR 49000, Risikomanagement für Organisationen und Systeme, Begriffe und Grundlagen," Austrian Standards plus GmbH, Wien, 2014.

[4] Austrian Standards Institute, „ONR 49001, Risikomanagement für Organisationen und Systeme, Risikomanagement," Austrian Standards plus GmbH, Wien, 2014.

[5] Austrian Standards Institute, „ONR 49002-1, Risikomanagement für Organisationen und Systeme, Teil 1: Leitfaden für die Einbettung des Risikomanagements ins Managementsystem," Austrian Standards plus GmbH, Wien, 2014.

[6] Austrian Standards Institute, „ONR 49002-2, Risikomanagement für Organisationen und Systeme, Teil 2: Leitfaden für die Methoden der Risikobeurteilung," Austrian Standards plus GmbH, Wien, 2014.

[7] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-3 Risikoanalyse auf Basis IT-Grundschutz," Bonn, 2017.

[8] DIN, „DIN EN 80001-1:2011-11: Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten," 2011.

[9] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)," Bonn, 2017.

[10] Deutsche Krankenhaus Gesellschaft, „Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus," Berlin, 2019.

[11] BSI, „www.bsi.bund.de," Bundesamt für Sicherheit in der Informationstechnik, [Online]. Available: https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_8aBSIG_allgemein/faq_bsi_8a_allgemein_node.html#faq10523112. [Zugriff am 25 Januar 2020].

[12] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT," Bonn, 2013.

[13] Bundesamt für Sicherheit in der Informationstechnik, „Hilfsmittel Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT," Bonn, 2015.

[14] Bundesamt für Sicherheit in der Informationstechnik, „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG Version 1.0," Bonn, 2017.

[15] Georg-August-Universität Göttingen, „Informationssicherheitsrichtlinie der Georg-August-Universität Göttingen," *Amtliche Mitteilungen der Georg-August-Universität Göttingen,* offen 2019.

Anlage 4 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.

Erhöhter Schutzbedarf

Zusammenfassende Bezeichnung für hoher oder sehr hoher Schutzbedarf im Gegensatz zu normalem Schutzbedarf.

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 Nutzungskonto, 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.

Nutzungskonto

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.

Nutzungskonto, privilegiertes

Spezielles Nutzungskonto, mit dem erhöhte Rechte im IT-System verbunden sind. Insbesondere werden darunter auch Nutzungskonten 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 Nutzungskonto überprüft wird, z.B. Passwörter und PINs, kryptographische Schlüssel oder biometrische Daten.