GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Richtlinie zur Informationssicherheit der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG)

– Informationssicherheitsrichtlinie (ISRL) –

Die Geschäftsführung der GWDG hat am 10.01.2022 die Neufassung der Richtlinie zur Informationssicherheit der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) beschlossen.

Die Zustimmung des Betriebsrats ist am 01.12.2021 erfolgt.

Inhaltsverzeichnis

Abschnitt I: Grundsätze

§ 1 Gegenstand und Geltungsbereich

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

(2) Die Informationssicherheitsrichtlinie gilt für alle Beschäftigten der GWDG insbesondere, wenn sie die IT-Infrastruktur der GWDG oder die von ihr im Auftrag anderer betriebene IT-Infrastruktur nutzen oder Daten der GWDG oder der Auftraggeber der GWDG verarbeiten, und für die gesamte IT-Infrastruktur der GWDG einschließlich der betriebenen IT-Systeme.

§ 2 Rahmenbedingungen

(1) Der Betrieb eines Rechenzentrums 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 GWDG als IT-Dienstleister 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 Informationssicherheitsrichtlinie für die GWDG 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 GWDG 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 GWDG verarbeiteten Daten und Anwendungen und die von ihr betriebene IT-Infrastruktur zu schützen sowie die GWDG 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 Nutzergruppen mit ihren unterschiedlichen Rollen und Rechten und die schnellen Entwicklungszyklen der Informationstechnik zu berücksichtigen.

(5) Die GWDG orientiert sich in dieser Richtlinie an den entsprechenden Richtlinien der Gesellschafter.

§ 3 Sicherheitsziele

(1) Im Sinne dieser Richtlinie ist Informationssicherheit die Herstellung und Aufrechterhaltung der

(a) „Vertraulichkeit“; das bedeutet, die Gewährleistung des Zugangs zu und Zugriffs auf Informationen nur für Berechtigte,

(b) „Integrität“; das bedeutet, die Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden,

(c) „Verfügbarkeit“; das bedeutet, die Gewährleistung des bedarfsorientierten Zugriffs auf Informationen für Berechtigte.

(2) Durch diese Informationssicherheitsrichtlinie soll sichergestellt werden, dass dem jeweiligen Schutzzweck angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um das Eintreten von Informationssicherheitsvorfällen weitestgehend zu minimieren. Die Maßnahmen dienen insbesondere

(a) der zuverlässigen Unterstützung der Prozesse durch die IT und der Sicherstellung der Kontinuität der Arbeitsabläufe,

(b) der Patientensicherheit und Behandlungseffektivität in der medizinischen Versorgung durch die Universitätsmedizin Göttingen,

(c) der Wahrung von Dienst-, Betriebs-, Geschäfts- und sonstigen Geheimnissen,

(d) der Gewährleistung der aus rechtlichen Vorgaben resultierenden Anforderungen,

(e) der Gewährleistung des informationellen Selbstbestimmungsrechts der oder des Betroffenen bei der Verarbeitung derer oder dessen personenbezogener Daten,

(f) der Einhaltung der Ordnungen der Gesellschafter 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 Kooperationspartnern.

§ 4 Informationssicherheitsprozess

(1) Der Informationssicherheitsprozess dient der Sicherheit der Daten, wobei die Sicherheit der datenverarbeitenden Systeme und Stellen gewährleistet werden muss, und umfasst insbesondere folgende Aufgaben:

(a) Verantwortlichkeiten zu definieren und festzulegen,

(b) den Schutzbedarf festzustellen und die Risiken zu erfassen,

(c) den Zugang zu und den Zugriff auf Informationen sowie Art und Umfang der Autorisierung zu definieren und festzulegen,

(d) Sicherheits- und Kontrollmaßnahmen entsprechend der Informationssicherheitsrichtlinie festzulegen,

(e) Sicherheits- und Kontrollmaßnahmen zum Schutz der Informationen umzusetzen, zu überprüfen und zu aktualisieren.

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

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

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

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

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

Verbleibende Risiken im Rahmen der Risikoakzeptanz sind zu beschreiben und durch die Geschäftsführung gemäß zu verantworten.

Abschnitt II: Organisatorische Festlegungen

§ 5 Geschäftsführung

(1) Die Gesamtverantwortung für die Informationssicherheit und den Informationssicherheitsprozess liegt bei der Geschäftsführung der GWDG.

(2) Geschäftsführung delegiert die Organisation und Durchführung des Informationssicherheitsmanagements in dem in § 7 und § 8 festgelegten Umfang auf die Informationssicherheitsbeauftragte oder den Informationssicherheitsbeauftragten (ISB) beziehungsweise auf die Informationssicherheitsmanagerinnen oder Informationssicherheitsmanager (ISM).

(3) Die Geschäftsführung ist verantwortlich für:

a) die Benennung von Fachverantwortlichen nach Absatz (4),

b) die Beschlussfassung über die jeweiligen Betriebskonzepte nach Absatz (5)

c) Entscheidung über die weitere Behandlung von Informationssicherheitsvorfällen nach § 13.

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

(5) Die Geschäftsführung beschließt nach Stellungnahme des ISB die Betriebskonzepte und verantwortet die in diesen Konzepten übernommen Risiken.

§ 6 Fachverantwortliche

(1) Fachverantwortliche sind bzgl. der ihnen zugeordneten Datenbeständen, IT-Verfahren, IT-Systeme und Infrastrukturen für die Umsetzung des Informationssicherheitsprozesses verantwortlich, was insbesondere die folgenden Aufgaben umfasst:

(a) Feststellung des Schutzbedarfs von Informationen, IT-Verfahren, IT-Systemen und Infrastrukturen sowie Analysierung der Risiken,

(b) Erstellung und Fortschreibung der Betriebskonzepte auf Basis von Schutzbedarfsfeststellung und Risikoanalyse,

(c) regelmäßige Überprüfung der Schutzbedarfsfeststellung, Risikoanalyse und des Betriebskonzepts entsprechend der im Betriebskonzept festzulegenden Intervallen,

(d) Veranlassung und Kontrolle der Umsetzung der Maßnahmen des Betriebskonzepts, insbesondere auch bei Inanspruchnahme externer IT-Dienstleister (z.B. Auftragsverarbeitung).

(2) Fachverantwortliche können zur Wahrnehmung ihrer Aufgaben die Beratung der oder des ISB oder anderer Beschäftigter der GWDG anfordern.

(3) Ergebnis einer Schutzbedarfsfeststellung und Risikoanalyse kann auch sein, dass für einen Datenbestand, ein IT-Verfahren, ein IT-System oder eine Infrastruktur über die Umsetzung der Informationssicherheitsrichtlinie und des Maßnahmenkatalogs für den IT-Grundschutz (0) hinaus keine weiteren Maßnahmen erforderlich sind.

§ 7 Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter (ISB)

(1) Die Geschäftsführung benennt 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 sowie die Überwachung der Umsetzung des Informationssicherheitsprozesses für die GWDG,

(b) Entwicklung von Empfehlungen für die Geschäftsführung für folgende Themenfelder:

(i) Erstellung und Fortschreibung des Maßnahmenkatalogs für den IT-Grundschutz,

(ii) ergänzende Informationen zur Informationssicherheitsrichtlinie (z. B. Empfehlungen für interne technische Standards, Musterlösungen, und Notfallpläne),

(iii) Änderungen zu Betriebskonzepten auf Grund von Sicherheitsvorfällen (im Sinne von § 13 Abs. (3)),

(iv) Schulungskonzepte.

(c) Beratung folgender Stellen:

(i) Geschäftsführung in Fragen der Informationssicherheit und bei der Umsetzung der Informationssicherheitsrichtlinie,

(ii) Datenschutzbeauftragte und Datenschutzmanagerinnen oder Datenschutzmanager bezüglich technischer und organisatorischer Maßnahmen,

(iii) Fachverantwortliche bei der Erstellung von Betriebskonzepten.

(d) Stellungnahme zu den Betriebskonzepten,

(e) Erstellung und Aktualisierung eines Verzeichnisses aller Betriebskonzepte,

(f) Bewertung von Informationssicherheitsvorfällen und Ableitung von strukturellen und konzeptionellen Empfehlungen gemäß § 13,

(g) Erstellung des jährlichen Berichts für die Geschäftsführung zur Informationssicherheit einschließlich Empfehlungen zur Überarbeitung dieser Informationssicherheitsrichtlinie und anderer übergreifender Informationssicherheitskonzepte; bei Bedarf erfolgt die Berichterstattung auch darüber hinaus.

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

§ 8 Informationssicherheitsmanagerin oder Informationssicherheitsmanager (ISM)

(1) Die Geschäftsführung benennt für die GWDG 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,

(b) Bewertung und Weiterleitung von Meldungen zu Informationssicherheitsvorfällen und Erstellung von Handlungsempfehlungen für die Behandlung der Informationssicherheitsvorfälle im operativen Bereich gemäß § 13 Abs. (2); Prüfung, ob eine Informationssicherheitsvorfall gleichzeitig auch eine Datenschutzvorfall sein könnte.

(c) Erstellung des Berichts zur Informationssicherheit, soweit es

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

(ii) Informationssicherheitsvorfälle

betrifft.

§ 9 Datenschutz- und Informationssicherheits-Koordinationsteam

(1) Das Datenschutz- und Informationssicherheits-Koordinationsteam (DIKT) besteht aus:

(a) der oder dem ISB der GWDG,

(b) der oder dem ISM der GWDG,

(c) der oder dem Datenschutzbeauftragten (DSB) der GWDG,

(d) der Datenschutzmanagerin oder dem Datenschutzmanager (DSM) der GWDG,

(e) den jeweiligen Stellvertreterinnen oder Stellvertretern der ISB, ISM, DSB und DSM,

(f) einem Vertreter der Geschäftsführung der GWDG,

(g) einem Mitglied des Betriebsrats der GWDG sowie

(h) weiteren von der Geschäftsführerin oder dem Geschäftsführer oder der oder dem ISB bei Bedarf benannten Personen.

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

(3) Das DIKT dient den folgenden Zwecken:

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

(b) Erarbeitung von Empfehlungen zur Änderung der Informationssicherheitsrichtlinie und übergreifender Konzepte und Empfehlungen zur Informationssicherheit und zum Datenschutz.

§ 10 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

§ 11 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.

§ 12 Zusätzliche Maßnahmen

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

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

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

§ 13 Umgang mit Informationssicherheitsvorfällen

(1) Beschäftigte der GWDG haben für die Informationssicherheit relevante Vorfälle (Informationssicherheitsvorfälle) unverzüglich der oder dem ISM mitzuteilen.

(2) Die oder der ISM bewertet die Schwere des Informationssicherheitsvorfalls und informiert die oder den ISB über den gemeldeten Informationssicherheitsvorfall und holt dessen Stellungnahme ein. Die oder der ISM informiert die Geschäftsführung 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. Informationssicherheitsvorfälle, die den Datenschutz betreffen, sind – nach ihrer Verabschiedung entsprechend der geltenden Datenschutzrichtlinie der GWDG – der oder dem DSM zu melden.

(3) Die Geschäftsführung entscheidet über die weitere Behandlung eines von der oder dem ISM an die Geschäftsführung gemeldeten Informationssicherheitsvorfalls.

(4) 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 der oder des ISM, im Falle von Datenschutzvorfällen auch der oder des DSB und der oder des DSM Empfehlungen für die Geschäftsführung.

(5) Die oder der ISM meldet Informationssicherheitsvorfälle an die zuständigen Behörden. Soweit Informationssicherheitsvorfälle zugleich Datenschutzvorfälle darstellen, erfolgt die Meldung an die hierfür zuständigen Behörden – nach ihrer Verabschiedung entsprechend der geltenden Datenschutzrichtlinie der GWDG – durch den DSM.

(6) Betrifft ein Informationssicherheitsvorfall Nutzungskonten oder IT-Systeme einer nutzungsberechtigten Institution, so sind die für die Behandlung von Informationssicherheitsvorfällen zuständigen Kontaktpersonen von der oder dem ISM zu informieren und in die Behandlung des Informationssicherheitsvorfalls einzubinden.

(7) Das Nähere zum Umgang mit Informationssicherheitsvorfällen kann die Geschäftsführung in einer Handlungsanweisung regeln.

§ 14 Gefahrenintervention

(1) Um eine gegenwärtige Gefahr für die Informationssicherheit abzuwehren, trifft das IT-Personal 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.

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

(3) Die oder der ISM ist unverzüglich zu informieren.

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

(5) Betreffen die ergriffenen Maßnahmen Nutzungskonten oder IT-Systeme einer nutzungsberechtigten Institution, so sind die für die Behandlung von Informationssicherheitsvorfällen zuständigen Kontaktpersonen von der oder dem ISM zu informieren und in die Behandlung des Informationssicherheitsvorfalls insbesondere auch bei Aufhebung von Maßnahmen einzubinden.

Schlussbestimmungen

In- und Außerkrafttreten

(6) Die Richtlinie zur Informationssicherheit der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) tritt am 10.01.202205.12.2023 in Kraft.

(7) Gleichzeitig tritt die IT-Sicherheitsleitlinie der GWDG vom 10.02.2004 außer Kraft.

Anlage 1: Maßnahmenkatalog für den IT-Grundschutz

A. Maßnahmen für Anwender

A.1 Anwenderqualifizierung

Verantwortlich für Initiierung:	Geschäftsführung
Verantwortlich für Umsetzung:	Vorgesetzte

(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:	ISM
Verantwortlich für Umsetzung:	alle Beschäftigten

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

A.3 Konsequenzen und Sanktionen bei Sicherheitsverstößen

Verantwortlich für Initiierung:	Geschäftsführung
Verantwortlich für Umsetzung:	Geschäftsführung

(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 Beschäftigten der GWDG, Nutzer, Vertragspartner, Berater in erheblichen Umfang beeinträchtigt wird,

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

(c) der GWDG oder nutzungsberechtigten Institutionen 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 GWDG oder nutzungsberechtigter Institutionen für illegale Zwecke ermöglicht wird und

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

(3) Liegen hinreichende 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 festzuhalten. Schon vor Maßnahmenbeginn sind die oder der zuständige Datenschutzbeauftragte und eine Vertretung des Betriebsrats (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:	ISM
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

(1) Auf IT-Systemen der GWDG darf nur Software installiert werden, die zur Erfüllung der dienstlichen 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:	ISM
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:	ISM
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 Abwe-

senheit zu verschließen. Hiervon darf nur abgewichen werden, soweit es die Arbeitsorganisation dringend erfordert und andere Sicherheitsmaßnahmen es ermöglichen.

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

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

A.7 Sperren und ausschalten

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

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

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

(3) Grundsätzlich sind die 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:	ISM
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:	ISM
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.

[1] Algorithmus, Schlüssellänge nach Angaben der Bundesnetzagentur

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

(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) 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:	ISM
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

(1) Jede Person ist für alle Handlungen verantwortlich, die unter Verwendung ihres Nutzungskontos vorgenommen werden.

(2) Die für Nutzung von IT-Systemen, die von der GWDG betrieben werden, verwendeten Passwörter (nachfolgend dienstliche Passwörter) dürfen nicht mit Passwörtern identisch oder ähnlich sein, die zur Nutzung von anderen, nicht von der GWDG betriebenen IT-Systemen verwendet 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 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 andere 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 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:	ISM
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. technisch mögliche aber verbotene Einsichtnahme in Daten von Benutzern durch Administratoren).

A.12 Netzzugänge

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

(1) Der Anschluss von IT-Systemen an das von der GWDG betriebene Datennetz 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:	Geschäftsführung
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 Betriebsvereinbarungen[2] sowie weitere Regelungen zum Datenschutz und zur Datensicherheit zu beachten.

A.14 Sichere Netzwerknutzung - Allgemeine Anforderungen

Verantwortlich für Initiierung:	ISM
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:	ISM
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 von Daten zu verwenden.

(4) Wird auf dienstliche E-Mails von außerhalb der GWDG / der von der GWDG betriebenen Netze 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 von der GWDG betriebenen 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 GWDG zu speichern.

[2] Siehe Anlage „Mitgeltende Dokumente“

(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 GWDG (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 GWDG ist nur in den Staaten des europäischen Wirtschaftsraums und sicheren Drittstaaten entsprechend dem Datenschutzrecht zulässig.

(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:	ISM
Verantwortlich für Umsetzung:	IT-Anwender

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

(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:	ISM
Verantwortlich für Umsetzung:	IT-Anwender

(1) Die Benutzung von privater Hard- und Software ist in Verbindung mit dienstlichen Daten oder der IT-Infrastruktur der GWDG nur erlaubt, wenn die Betriebskonzepte für den jeweiligen Datenbestand und Teilbereich der Infrastruktur 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 GuestOn-Campus der GWDG.

(3) Die Zulassung von privaten Geräten in anderen Teilen der Infrastruktur der GWDG setzt zwingend voraus, dass dort angeschlossene Endgeräte den Anforderungen der Maßnahmenkataloge zum IT-Grundschutz der GWDG 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 ISM zu informieren. Sind personenbezogene Daten vom Verlust betroffen, ist zusätzlich die oder der DSM zu informieren.

A.19 Datensicherung und Archivierung

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

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

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

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

(4) Von der Datensicherung zum Schutz vor Verlust ist die 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 anderen geeigneten technischen Maßnahmen (z.B. mit einem Gerät zum magnetischen Durchflutungslöschen für Festplatten und Magnetbänder) 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 Regelungen der GWDG und die Anforderungen der nutzungsberechtigten Institutionen zu beachten.

(5) Weitere Informationen können beim Datenschutzbeauftragten der GWDG bei der Arbeitsgruppe Nutzerservice und Betriebsdienste erfragt werden.

I. Maßnahmen für IT-Personal

I.1 Frühzeitige Berücksichtigung von Informationssicherheitsfragen

Verantwortlich für Initiierung:	Geschäftsführung
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 sollten 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:	Geschäftsführung
Verantwortlich für Umsetzung:	Fachverantwortliche

(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:	ISM
Verantwortlich für Umsetzung:	IT-Personal, IT-Anwender

(1) Informationssicherheitsereignisse und -vorfälle sind vom zuständigen IT-Personal zu dokumentieren und die oder dem ISM 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 GWDG durch andere oder durch die GWDG im Auftrag anderer 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 GWDG ist einzubeziehen.

I.6 Standards für technische Ausstattung und Konfiguration

Verantwortlich für Initiierung:	Geschäftsführung
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 fachlich qualifiziertes IT-Personal der GWDG beraten die Betreiber der IT-Verfahren.

I.7 Bereitstellung zentraler IT-Dienste

Verantwortlich für Initiierung:	Geschäftsführung
Verantwortlich für Umsetzung:	Fachverantwortliche

(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.

(4) Betreibt die GWDG IT-Systeme im Auftrag Dritter oder stellt im Rahmen von Hosting oder Housing Möglichkeiten zum Betrieb von IT-Systemen Dritten in der Infrastruktur der GWDG zur Verfügung, so ist bei den vertraglichen Regelungen die Umsetzung dieser Informationssicherheitsrichtlinie und ergänzender Regelungen der GWDG zur Informationssicherheit anzustreben. Abweichungen sind gegebenenfalls bei Auftragsübernahme schriftlich festzulegen.

I.8 Nutzung zentraler Dienste

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

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

(2) Die Beschäftigten der GWDG sollen auf zentrale IT-Dienste 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:	Geschäftsführung / Fachverantwortliche
Verantwortlich für Umsetzung:	Geschäftsführung

(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:	Geschäftsführung / Fachverantwortliche
Verantwortlich für Umsetzung:	Geschäftsführung

(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:	Geschäftsführung
Verantwortlich für Umsetzung:	Sicherheitsbeauftragter

(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 beim Sicherheitsbeauftragten der GWDG und den zuständigen Stellen der Vermieter. 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:	ISM
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.

I.13 Sicherung der Netzknoten

Verantwortlich für Initiierung:	Gebäudemanagement
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.

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

I.14 Verkabelung und Funknetze

Verantwortlich für Initiierung:	Geschäftsführung
Verantwortlich für Umsetzung:	Fachverantwortliche

(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 über die Arbeitsgruppe IT-Infrastruktur einzureichen.

I.15 Einweisung und Beaufsichtigung von Fremdpersonal

Verantwortlich für Initiierung:	ISM
Verantwortlich für Umsetzung:	Fachverantwortliche

(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, 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:	ISM
Verantwortlich für Umsetzung:	Fachverantwortliche

(1) Die Beschaffung von Soft- und Hardware und die Entwicklung von Software sind mit der oder dem zuständigen ISB 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:	ISM
Verantwortlich für Umsetzung:	IT-Personal

(1) Auf IT-Systemen der GWDG 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:	ISM
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:	ISM
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 ISM 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 E-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:	ISM
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:	ISM
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:	ISM
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 und Freigabe eines Nutzungskontos darf nur in einem geregelten Verfahren erfolgen. Die Einrichtung und Freigabe ist zu dokumentieren.

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

I.24 Administratorkonten

Verantwortlich für Initiierung:	ISM
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:	Geschäftsführung
Verantwortlich für Umsetzung:	Geschäftsführung, 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 Geschäftsführung 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:	ISM
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 sollten 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 die Möglichkeit bereitgestellt werden, unterschiedliche Passwörter oder Authentifizierungsverfahren einzusetzen.

(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:	Geschäftsführung
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:	ISM
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:	Geschäftsführung
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 vorhandene Anforderungen an die Revisionssicherheit erfüllt.

(3) Zur Einrichtung und zum Betrieb von externen Arbeitsplätzen sind die bestehenden Betriebsvereinbarungen[4] zu beachten.

(4) Werden bei der externen Arbeit personenbezogene Daten verarbeitet, muss die bzw. der zuständige Datenschutzbeauftragte im Genehmigungsprozess hinzugezogen werden.

I.30 Notwendigkeit von Protokollierung und Monitoring

Verantwortlich für Initiierung:	ISM / 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 und dem Betriebsrat abzustimmen.

[4] Siehe Anlage Mitgeltende Dokumente

I.31 Protokollierung auf Servern und bei Anwendungsprogrammen

Verantwortlich für Initiierung:	ISM / 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:	ISM
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:	ISM
Verantwortlich für Umsetzung:	IT-Personal

(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:	ISM
Verantwortlich für Umsetzung:	IT-Personal

(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:	ISM
Verantwortlich für Umsetzung:	IT-Personal

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

I.36 Aufteilungen in Bereiche unterschiedlichen Schutzbedarfs

Verantwortlich für Initiierung:	ISM
Verantwortlich für Umsetzung:	Fachverantwortliche

(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:	ISM
Verantwortlich für Umsetzung:	Fachverantwortliche

(1) Die gesamte Kommunikation zwischen verschiedenen Teilnetzen der GWDG 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 GWDG 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:	ISM
Verantwortlich für Umsetzung:	Fachverantwortliche

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

(2) Schützenswerte Daten sind zwingend verschlüsselt zu übertragen.

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

I.39 Organisation der Datensicherung

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

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

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

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

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

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

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

I.40 Anwenderinformation zur Datensicherung

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

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

I.41 Verifizierung der Datensicherung

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

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

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 Management

V.1 Überprüfung bei Personaleinstellung

Verantwortlich für Initiierung: Verantwortlich für Umsetzung:

(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: Verantwortlich für Umsetzung:

(1) Nach der Einstellung ist unverzüglich sicher zu stellen, das neu eingestelltes Personal in die Informationssicherheitsrichtlinie eingewiesen und darauf verpflichtet ist.

(2) Es ist sicher zu stellen, dass 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 sollten 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: Verantwortlich für Umsetzung:

(1) Grundlegende Schulung zur Informationssicherheit sollten 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: Verantwortlich für Umsetzung:

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

(2) Vertretungsregelungen sind zu dokumentieren.

Anlage 2: Mitgeltende Dokumente

- Betriebsvereinbarung über Mobiles Arbeiten (s. https://www.gwdg.de/about-us/company-internal-regulations/mobile-working)
- Netzbetriebsordnung der Universitätsmedizin (s. https://it.umg.eu/de/media/content/NETZE_betriebshandbuch_netzbetriebsordnung.pdf)
- Nutzungsordnung der GWDG (s. https://www.gwdg.de/web/guest/about-us/catalog/terms-and-conditions/terms-of-use)
- Hausordnung der GWDG (https://sharepoint.gwdg.de/Allgemeine%20Dokumente/Betriebsordnung%2C%20Hausordnung%2C%20Verhaltensregeln/Hausordnung_GWDG_2014_10_02_gez.pdf)
- Betriebsordnung der GWDG (https://sharepoint.gwdg.de/Allgemeine%20Dokumente/Betriebsordnung%2C%20Hausordnung%2C%20Verhaltensregeln/Betriebsordnung_2013_07_01.pdf)
- Genehmigte Software / Approved Software (https://doku.it-goettingen.de/x/VB_7Ag)

Im Dokumentenlenkungssystem Roxtra (https://qms.gwdg.de) hinterlegte Dokumente:

- Aktionskarte
- Analyse und Spezifikation von Informationssicherheitsanforderungen
- Berechtigung Lokale Administrationsrechte
- Entsorgungsrichtlinie der GWDG
- Ergänzende Absprachen und Erläuterungen zur Informationssicherheitsrichtlinie
- Handlungsanweisung_Informationssicherheitsvorfälle
- Kompetenzprofile
- Konzept Netzwerksicherheitsmanagement
- Konzept Schulung und Sensibilisierung
- Konzept Schwachstellenmanagement
- Regeln Softwareinstallation
- Richtlinie Dienstleister- und Lieferantenbeziehungen
- Richtlinie für ein aufgeräumte Arbeitsumgebung und Bildschirmsperren
- Richtlinie Gebrauch kryptographischer Maßnahmen
- Richtlinie Informationsklassifizierung
- Richtlinie Mobilgeräte
- Richtlinie zur Entsorgung von Datenträgern
- Richtlinie zur Informationsübertragung
- Richtlinie_Sichere-Entwicklung
- RL Administrationstätigkeiten
- RL Audits von Informationssystemen
- RL Changemanagement
- RL Datensicherung
- RL Ereignisprotokollierung
- RL Informationssicherheitsvorfälle
- RL Inventarisierung
- RL Mobiles Arbeiten und private Hard- und Software
- RL Schutz_vor_Schadsoftware
- RL Zugangssteuerung
- RL_Clientmanagement
- RL_Testmanagement
- RL-Informationssicherheits-Risikomanagement
- Verfahrensanweisung Handhabung von Datenträgern
- Vorgaben-Projektmanager-Informationssicherheit
- Vorgehen bei internen Sicherheitsverstößen

Anlage 3: Glossar

Anwendung

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

Anwendungsserver

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

Datenbestand

Eine Menge von digital gespeicherten Daten.

Datenarchivierung

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

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

Datensicherung

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

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

Datenspeicherung

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

Datenträger

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

Erhöhter Schutzbedarf

Zusammenfassung 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.

Hosting

Betrieb virtueller IT-Systeme (Guests) Dritter auf IT-Systemen (Hosts) der GWDG.

Housing

Betrieb physischer IT-Systeme Dritter in der IT-Infrastruktur der GWDG.

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 Beschäftigten der GWDG, 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 GWDG mit der Installation und dem Betrieb von Datennetzen betraute Gruppen und deren Mitarbeiter.

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.

Rechner

Abgrenzung Server ⇔ Desktop/Notebook sinnvoll, oder „Rechner“ im Dokument konsequent durch die tatsächlich gemeinten Systeme ersetze

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.