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

– Informationssicherheitsrichtlinie (ISRL) –

Die Geschäftsführung der GWDG hat am 30.09.2025 die Neufassung der Richtlinie zur Informationssicherheit der Gesellschaft für wissenschaftliche Datenverarbeitung Göttingen mbH (GWDG) beschlossen.

Die Zustimmung des Betriebsrats ist am 26.09.2025 erfolgt.

Inhaltsverzeichnis

Abschnitt I: Grundsätze

§ 1 Gegenstand und Geltungsbereich

(1) Die Informationssicherheitsrichtlinie legt Verantwortungsstrukturen, Aufgabenzuordnung und Zusammenarbeit der Beteiligten und 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 Nutzendengruppen 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 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 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, Informationssicherheitsmanagementsystem und Informationssicherheits-Risikomanagement

(1) Der durch das Informationssicherheitsmanagementsystem gesteuerte 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 zu verantworten.

(4) Die Richtlinie zum Informationssicherheits-Risikomanagement 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 der Maßnahmenkataloge für den IT-Grundschutz nach § 15 eine weitere Risikoanalyse nicht erforderlich.

Abschnitt II: Organisatorische Festlegungen

§ 5 Geschäftsführung

(1) Die Gesamtverantwortung für die Informationssicherheit, das Informationssicherheitsmanagementsystem und den Informationssicherheitsprozess liegt bei der Geschäftsführung der GWDG. Die Gesamtverantwortung schließt die Verantwortung für das Informationssicherheits-Risikomanagement entsprechend der Richtlinie zum Informationssicherheits-Risikomanagement ein.

(2) Geschäftsführung delegiert 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) Die Leitung der Arbeitsgruppen der GWDG (nachfolgend: Gruppenleitung, GL) obliegt in ihren Arbeitsgruppen die Wahrnehmung der in § 8 festgelegten Aufgaben. Die Geschäftsführung kann die Delegation nach Satz 1 aufheben und selbst entscheiden.

(4) Die Geschäftsführung ist verantwortlich für die Entscheidung über die weitere Behandlung von Informationssicherheitsvorfällen nach § 17.

§ 6 Gruppenleitungsbesprechung (GLB)

(1) Regelmäßige, i. d. R. wöchentliche, Besprechungen der Geschäftsführung und der Gruppenleitungen dienen der Beratung und Abstimmung von strategischen Fragen.

(2) Entscheidungsbefugnisse liegen bei der Geschäftsführung.

§ 7 Zusammenarbeit der IT-Dienstleister am Campus

(1) Die GWDG stimmt strategische Fragen einschließlich grundsätzlicher Fragen der Informationssicherheit im Rahmen der Kooperation GÖ* mit den anderen IT-Dienstleistern der Georg-August-Universität Göttingen ab.

(2) Entscheidungsbefugnisse verbleiben für die Tätigkeiten der GWDG bei der Geschäftsführung der GWDG.

§ 8 Gruppenleitungen (GL)

(1) Die Gruppenleitung ist in der jeweiligen Arbeitsgruppe verantwortlich für:

a) die Benennung einer Informationssicherheitskoordinatorin oder eines Informationssicherheitskoordinators nach Absatz (2),

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

c) die Beschlussfassung über die jeweiligen Betriebskonzepte nach Absatz (5),

d) die Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß der Richtlinie zum Informationssicherheits-Risikomanagement.

(2) Die Gruppenleitung kann für die jeweilige Arbeitsgruppe eine Beschäftigte oder einen Beschäftigten der Arbeitsgruppe als Informationssicherheitskoordinatorin oder Informationssicherheitskoordinator (ISK) benennen. Die Benennung ist zu dokumentieren. Wird keine oder kein ISK benannt, obliegen deren oder dessen Gruppenleitung. Die Gruppenleitung kann für die oder den ISK auch eine oder mehrere Stellvertretungen benennen.

(3) Die Gruppenleitungen mehrerer Arbeitsgruppen können einvernehmlich für ihre Arbeitsgruppen gemeinsame ISK benennen.

(4) Für die einer Arbeitsgruppe zugeordneten Informationswerten, Datenbeständen, IT-Verfahren, IT-Systeme und Infrastrukturen kann die Gruppenleitung 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 Gruppenleitung.

(5) Die Gruppenleitung beschließt nach Stellungnahme des ISK und Zustimmung des ISB die Betriebskonzepte und Risikoanalysen einschließlich der nach Überprüfungen überarbeiteten Fassungen und verantwortet die in diesen Betriebskonzepten und Risikoanalysen 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 Gruppenleitung.

(2) Die Gruppenleitung ist dafür verantwortlich, dass die ISK mit den für die Erfüllung ihrer Aufgaben erforderlichen Befugnissen und Ressourcen ausgestattet sind. Die Gruppenleitung 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) Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß Richtlinie zum Informationssicherheits-Risikomanagement.

(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 Informationswerte, Datenbestände, 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,

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

(2) (2) Den Fachverantwortlichen obliegt zudem die Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß der Richtlinie zum Informationssicherheits-Risikomanagements

(3) Fachverantwortliche können zur Wahrnehmung ihrer Aufgaben die Beratung der oder des ISK, der oder des ISB oder anderer Beschäftigter der GWDG 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 der Maßnahmenkataloge für den IT-Grundschutz nach § 15 hinaus keine weiteren Maßnahmen erforderlich sind.

§ 11 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 des Informationssicherheitsprozesses und des Informationssicherheitsmanagementsystems für die GWDG,

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

(i) Erstellung und Fortschreibung der Maßnahmenkataloge für den IT-Grundschutz nach *§ 15,*

(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 § 17 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) Arbeitsgruppen bei der Umsetzung der Informationssicherheitsrichtlinie,

(iv) ISK bei der Beseitigung von Gefahren für die Informationssicherheit,

(v) Fachverantwortliche bei der Erstellung von Betriebskonzepten.

(d) Zustimmung zu den Betriebskonzepten der Arbeitsgruppen einschließlich der nach Überprüfung durch die Fachverantwortlichen überarbeiteten Fassungen; im Dissensfall entscheidet die Geschäftsführung,

(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 die Geschäftsführung 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 der Richtlinie zum Informationssicherheits-Risikomanagement.

(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.

§ 12 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 § 17 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.

(d) Wahrnehmung der Aufgaben im Rahmen des Informationssicherheit-Risikomanagements gemäß der Richtlinie zum Informationssicherheits-Risikomanagement.

§ 13 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) den ISKs der Arbeitsgruppen,

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

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

(3) 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.

(4) Das DIKT dient den folgenden Zwecken:
   (a) Informationsaustausch und Abstimmung zwischen den am Informationssicherheitsprozess und am Datenschutzprozess Beteiligten,
   (b) Einbindung der Arbeitsgruppen in den Informationssicherheitsprozess,
   (c) Beratung der oder des ISB, der DSB sowie der oder des ISM und der oder des DSM in Fragen der Informationssicherheit und des Datenschutzes,
   (d) Erarbeitung von Empfehlungen zur Änderung der Informationssicherheitsrichtlinie und übergreifender Konzepte und Empfehlungen zur Informationssicherheit und zum Datenschutz.

§ 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 Maßnahmenkataloge für den IT-Grundschutz

(1) Für IT-Systeme mit normalem Schutzbedarf werden in den Maßnahmenkatalogen für den IT-Grundschutz (s. Anlage 1 Mitgeltende Dokumente) allgemein oder durch bestimmte Zielgruppen anzuwendende Maßnahmen definiert.

(2) Die Bestimmungen in den Maßnahmenkatalogen sind verbindlich; von ihnen kann ausschließlich nach Maßgabe von Absatz (3) abgewichen werden.

(3) Von den Maßnahmenkatalogen 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.

(4) Bei der Verarbeitung von personenbezogenen Daten sind die gesetzlichen und internen Vorgaben zum Datenschutzes zu berücksichtigen und gegeben falls zusätzlich technische und organisatorische Maßnahmen zu prüfen und umzusetzen.

§ 17 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 für die zuständige Stelle.

(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 entsprechend der geltenden Datenschutzrichtlinie der GWDG.

(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.

§ 18 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. 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 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

(1) Die Richtlinie zur Informationssicherheit der Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GWDG) tritt am 30.09.2025 in Kraft.

(2) Gleichzeitig tritt die Richtlinie zur Informationssicherheit der Gesellschaft für wissenschaftliche Datenverarbeitung mbH (GWDG)vom 11.01.2022 außer Kraft.

Anlage 1 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
- Maßnahmenkatalog für den IT-Grundschutz – Maßnahmen für Anwender
- Maßnahmenkatalog für den IT-Grundschutz – Maßnahmen für IT-Personal
- Maßnahmenkatalog für den IT-Grundschutz – Maßnahmen für Verwaltung und Management
- 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 2 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.

Daten mit besonderem Schutzbedarf

Daten mit besonderem Schutzbedarf im Sinne dieser Informationssicherheitsrichtlinie sind insbesondere

- personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO (z. B. Studierendendaten, Personaldaten, Patientendaten), die eine besondere Beeinträchtigung von Betroffenen bei einer unberechtigten Offenlegung oder sonstigen unberechtigten Verarbeitung erwarten lassen.
- Vertrauliche Unternehmensdaten (z.B. Finanzdaten, vertrauliche interne Informationen/Protokolle),
- Daten, die für die Anmeldungen von Patenten benötigt werden sowie
- im Einzelfall weitere Daten, die von einer IT-Anwenderin oder einem IT-Anwender als Daten mit besonderem Schutzbedarf eingestuft wurden (z. B. Forschungsergebnisse).

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.

Datenschutz

Datenschutz bedeutet den Schutz des Rechts auf informationelle Selbstbestimmung durch den Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten.

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.

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.

Informationssicherheit

Informationssicherheit bedeutet den Schutz von Informationen und Informationssystemen, um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen herzustellen und aufrechtzuerhalten (vgl. § 3(1)).

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 in den Maßnahmenkatalogen 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-Grundschutz

IT-Grundschutz bedeutet im Rahmen dieses Dokuments den Schutz von IT-Systemen mit normalem Schutzbedarf (im Gegensatz zu über den Grundschutz hinausgehenden Maßnahmen bei einem erhöhten Schutzbedarf). IT-Grundschutz wird hier nicht im Sinne der Umsetzung des IT-Grundschutzkompendiums des BSI verstanden.

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.

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.