

Kurzfassung der Richtlinie zur Informationssicherheit der Gesellschaft für wissen- schaftliche Datenverarbei- tung mbH Göttingen (GWGD)

Dies ist die Kurzfassung der Richtlinie zur Informationssicherheit der GWGD in der Fassung vom 10.01.2022. Dieses Dokument dient ausschließlich dazu, Kund*innen und anderen interessierten Parteien, der GWGD einen Überblick über die in der Richtlinie zur Informationssicherheit behandelten Themen zu geben. Bindend ist nur die Richtlinie selbst.

1. Verpflichtung zur Informationssicherheit

Die **GWGD** (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen) erklärt ihre umfassende Verpflichtung zur Sicherstellung und Förderung der Informationssicherheit. Dies schließt den Schutz von Informationen, IT-Systemen und -Prozessen ein, die zur Unterstützung ihrer Tätigkeiten in Forschung, Lehre, Gesundheitswesen und weiteren Bereichen eingesetzt werden. Die GWGD erkennt an, dass sichere IT-Prozesse die Grundlage für alle Aktivitäten der Organisation sind und für den Erhalt ihrer Leistungsfähigkeit essentiell sind.

Informationssicherheit ist ein zentrales strategisches Element für die GWGD, das sich nicht nur an gesetzlichen Anforderungen orientiert, sondern auch darauf abzielt, die GWGD vor materiellen und immateriellen Schäden zu bewahren.

2. Geltungsbereich

Die Informationssicherheitsrichtlinie gilt für alle Mitarbeitenden, Dienstleister und Partner, die die IT-Infrastruktur der GWGD nutzen oder auf Informationen der GWGD und ihrer Auftraggeber zugreifen. Sie umfasst die gesamte IT-Infrastruktur der GWGD, einschließlich aller betriebenen IT-Systeme und der verarbeiteten Daten.

Die Richtlinie deckt alle Bereiche der Informationssicherheit ab, darunter:

- Schutz der Daten und Systeme
- Risikomanagement und Risikobehandlung
- Incident Management (Behandlung von Sicherheitsvorfällen)
- Rollen und Verantwortlichkeiten in der Informationssicherheit.

3. Ziele der Informationssicherheit

Die GWGD hat sich folgende Sicherheitsziele gesetzt:

- **Vertraulichkeit:** Informationen sollen nur berechtigten Personen zugänglich sein.
- **Integrität:** Informationen und die genutzten Verarbeitungssysteme müssen korrekt und vollständig sein.
- **Verfügbarkeit:** Berechtigte Personen müssen Informationen jederzeit und bedarfsgerecht abrufen können.

Darüber hinaus zielt die GWGD darauf ab, ihre IT-Systeme so zu gestalten, dass sie sowohl die Anforderungen des Datenschutzes als auch die Grundsätze der guten wissenschaftlichen Praxis unterstützen.

4. Informationssicherheitsprozess und Maßnahmen

Die **GWGD** implementiert einen kontinuierlichen **Informationssicherheitsprozess**, um sicherzustellen, dass der Schutz von Informationen und Systemen stets gewährleistet ist. Dieser Prozess beinhaltet die folgenden Schritte:

- **Rollen und Verantwortlichkeiten:** Klare Definition der Aufgaben und Zuständigkeiten für die Informationssicherheit, einschließlich der Benennung eines Informationssicherheitsbeauftragten (ISB) und eines Informationssicherheitsmanagers (ISM).

- **Risikomanagement:** Die GWGD führt regelmäßige Risikoanalysen durch, um potenzielle Bedrohungen für ihre Informationsressourcen zu identifizieren. Auf Basis dieser Analysen werden Schutzmaßnahmen entwickelt und umgesetzt. Risiken werden kategorisiert nach „normalem“, „hohem“ oder „sehr hohem“ Schutzbedarf.
- **Sicherheits- und Kontrollmaßnahmen:** Sicherheitsmaßnahmen werden in einem Maßnahmenkatalog festgelegt, der sich am „IT-Grundschutz“ orientiert. Diese Maßnahmen betreffen sowohl IT-Anwender als auch IT-Personal und umfassen den kontrollierten Einsatz von Software, Virenschutz, Zugangskontrollen und regelmäßige Schulungen der Mitarbeitenden.

5. Verantwortlichkeiten

Die oberste Leitung der GWGD trägt die Gesamtverantwortung für die Informationssicherheit. Diese Verantwortung wird an den ISB und den ISM delegiert, die den Informationssicherheitsprozess koordinieren, weiterentwickeln und überwachen. Sie sind auch verantwortlich für die Erstellung von Empfehlungen zur Weiterentwicklung der Sicherheitsmaßnahmen und zur Behandlung von Sicherheitsvorfällen.

Fachverantwortliche für bestimmte IT-Systeme und Datenbestände tragen ebenfalls Verantwortung für die Implementierung und Überprüfung von Sicherheitsmaßnahmen im Rahmen der festgelegten Schutzerfordernungen.

6. Schulung und Sensibilisierung

Um die Einhaltung der Sicherheitsrichtlinie sicherzustellen, führt die GWGD regelmäßige Schulungen für alle Mitarbeitenden durch. Diese Schulungen sollen das Bewusstsein für Informationssicherheit stärken und sicherstellen, dass alle Mitarbeitenden die notwendigen Fähigkeiten haben, um sicher mit den IT-Systemen der GWGD umzugehen. Schwerpunkte der Schulungen sind:

- Sicherer Umgang mit IT-Systemen
- Sensibilisierung für Sicherheitsrisiken und Datenschutz
- Verfahren bei IT-Problemen und Sicherheitsvorfällen.

7. Behandlung von Sicherheitsvorfällen

Alle Mitarbeitenden der GWGD sind verpflichtet, Informationssicherheitsvorfälle unverzüglich zu melden. Die Bewertung und Bearbeitung solcher Vorfälle obliegt dem ISM in Abstimmung mit dem ISB. Die Geschäftsführung entscheidet über die weitere Vorgehensweise, insbesondere bei schwerwiegenden Vorfällen.

Zusätzlich gibt es klar definierte Maßnahmen zur **Gefahrenintervention**, falls akute Bedrohungen für die Informationssicherheit auftreten. IT-Personal ist befugt, notwendige Schritte zur Abwehr von Gefahren zu ergreifen, wie z. B. das Sperren von Netzanschlüssen oder Nutzungskonten.

8. Überwachung und kontinuierliche Verbesserung

Die GWGD überwacht kontinuierlich ihre Sicherheitsmaßnahmen, um deren Wirksamkeit sicherzustellen. Der ISB erstellt jährlich einen **Bericht zur Informationssicherheit**, in dem Fortschritte und Verbesserungsmöglichkeiten dokumentiert werden. Die GWGD verpflichtet sich, ihre Informationssicherheitsrichtlinie regelmäßig zu überprüfen und bei Bedarf anzupassen, um den neuesten Bedrohungen und Entwicklungen gerecht zu werden.

9. Zusammenarbeit mit externen Dienstleistern

Externe IT-Dienstleister, die im Auftrag der GWGD arbeiten, sind ebenfalls verpflichtet, die Informationssicherheitsrichtlinie der GWGD einzuhalten. Dies wird durch vertragliche Vereinbarungen sichergestellt. Die Einhaltung der Richtlinie wird regelmäßig überprüft, um sicherzustellen, dass keine zusätzlichen Risiken durch externe Partner entstehen.