



Leitlinie Informationssicherheit der kantonalen Verwaltung V2.0

Dokumentenhistorie

V1.0	26.04.2022	Ersterstellung
V2.0	21.04.2026	Überarbeitung

Inhaltsverzeichnis

1.	Zweck und Zielsetzung	4
2.	Geltungsbereich	4
3.	Normative Grundlage und Referenzen.....	4
4.	Abkürzungsverzeichnis	4
5.	Grundsätze der Informationssicherheit	4
6.	Ziele des ISMS	4
7.	Organisation und Verantwortlichkeiten	5
8.	Risikomanagement	5
9.	Sicherheitsmassnahmen	5
10.	Zusammenarbeit und kontinuierliche Verbesserung	5
11.	Inkrafttreten.....	6

1. Zweck und Zielsetzung

Diese Leitlinie legt den verbindlichen Rahmen für die Informationssicherheit innerhalb der kantonalen Verwaltung, Solothurn fest.

Sie dient dem Schutz von Informationen vor Verlust, Missbrauch, Manipulation und unbefugtem Zugriff und stellt die Einhaltung der geltenden gesetzlichen, regulatorischen, kantonalen und vertraglichen Anforderungen sicher.

2. Geltungsbereich

Die Leitlinie gilt für sämtliche Organisationseinheiten und Mitarbeitenden der kantonalen Verwaltung Solothurn, gemäss «IKT-Strategie 2021-2026 Kanton Solothurn».

Bei der Zusammenarbeit mit Dritten (Kunden, Partner, Dienstleistungsunternehmen, Lieferanten etc.) müssen die zur Informationssicherheit definierten Sicherheitsstandards so weit als möglich vertraglich eingebunden werden.

3. Normative Grundlage und Referenzen

Diese Leitlinie basiert auf

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Informations- und Datenschutzgesetz (InfoDG)
- Informations- und Datenschutzverordnung (InfoDV)
- IKT-Strategie 2021-2026 des Kantons Solothurn
- Digitalisierungsstrategie des Kantons Solothurn
- IKT-Governance des Kantons Solothurn

4. Abkürzungsverzeichnis

ISMS	Informationssicherheitsmanagement-System
IKT	Informations- und Kommunikationstechnologie
ISO	International Organization for Standardization
AIO	Amt für Informatik und Organisation
ISV	Informationssicherheitsverantwortliche/r
ODI	Operatives Führungsgremium Digitale Transformation & IKT
SDI	Strategisches Führungsgremium Digitale Transformation & IKT

5. Grundsätze der Informationssicherheit

Die Informationssicherheit gewährleistet übergeordnet die Sicherstellung folgender Schutzziele:

- **Vertraulichkeit:** Informationen sind nur für Berechtigte zugänglich.
- **Integrität:** Informationen sind korrekt, vollständig und unverändert.
- **Verfügbarkeit:** Sicherstellung der Verfügbarkeit von Informationen und Systemen bei Bedarf.
- **Nachvollziehbarkeit:** Sicherheitsrelevante Handlungen sind protokolliert.

6. Ziele des ISMS

- a. Schutz der Informationen der Bevölkerung, Partner und Mitarbeitenden.
- b. Minimierung von Sicherheitsrisiken.

- c. Sicherstellung der Gesetzeskonformität
- d. Etablierung eines kontinuierlichen Verbesserungsprozesses
- e. Erhöhung des Sicherheitsbewusstseins

7. Organisation und Verantwortlichkeiten

Dienststellen

Alle Dienststellen sind verantwortlich für die Sicherstellung der Informationssicherheit in ihrem eigenen Zuständigkeitsbereich. Sie definieren und regeln die spezifischen Anforderungen und Massnahmen entsprechend den Vorgaben und Standards der kantonalen Verwaltung und sorgen für die Umsetzung in ihrem Bereich.

Amt für Informatik und Organisation (AIO)

Das AIO betreibt für die von ihm bereitgestellten Services ein zertifiziertes Informationssicherheits-Managementsystem (ISMS) gemäss ISO 27001. Es legt verbindliche Standards und Vorgaben für den sicheren Betrieb dieser Services fest und stellt deren kontinuierliche Weiterentwicklung sicher. Darüber hinaus berät und unterstützt das AIO die Dienststellen in Fragen der Informationssicherheit und stellt Hilfsmittel, Prozesse und Schulungsangebote zur Verfügung.

ISV-Gremium

Das Gremium der Informationssicherheitsverantwortlichen (ISV), unter der Leitung des AIO, ist das zentrale Organ für den bereichsübergreifenden Austausch und die Koordination der Informationssicherheitsthemen in der kantonalen Verwaltung. Es setzt sich aus Vertretenden des Informationssicherheitsteams des AIO sowie den verantwortlichen Personen der Dienststellen zusammen. Das Gremium fördert die Harmonisierung, behandelt bereichsübergreifende Fragestellungen und unterstützt die Dienststellen in ihrer Aufgabe.

IKT-Governance

Die Steuerung der Digitalisierungs- sowie der IKT-Strategie der kantonalen Verwaltung ist integraler Bestandteil der IKT-Governance des Kantons Solothurn. Die operative und strategische Führung erfolgt durch die zuständigen Gremien ODI und SDI im Kontext der digitalen Transformation. Strategische übergeordnete Informationssicherheitsthemen werden ebenfalls unter dem Kontext der IKT-Governance verwaltet.

8. Risikomanagement

Das AIO führt ein systematisches Risikomanagement durch:

- Identifikation von Informationswerten
- Bewertung von Risiken
- Auswahl und Umsetzung von Sicherheitsmassnahmen
- Regelmässige Überprüfung

9. Sicherheitsmassnahmen

Die Massnahmen orientieren sich an den Kontrollen aus ISO/IEC 27002, u.a.

- Zugriffskontrolle
- Kryptografie
- Betriebssicherheit
- Lieferantenmanagement
- Incident Management
- Business Continuity

10. Zusammenarbeit und kontinuierliche Verbesserung

Die Zusammenarbeit zwischen Dienststellen, AIO und ISV-Gremium gewährleistet, dass Informationssicherheit nachhaltig verankert, laufend überprüft und an neue Anforderungen und Entwicklungen

angepasst wird. Die kontinuierliche Verbesserung des ISMS ist integraler Bestandteil der Sicherheitskultur.

Das ISMS wird durch:

- Interne/externe Audits
- Management Reviews
- Korrektur- und Verbesserungsmaßnahmen

kontinuierlich weiterentwickelt.

11. Inkrafttreten

Diese Leitlinie tritt am 21.04.2026 in Kraft und ersetzt die Version V1.0.