KANTON solothurn

Regierungsratsbeschluss

vom 22. September 2026

Nr. 2026/1638

Aufbau des Informationssicherheitsmanagementsystems (ISMS) der Verwaltung und der Gerichte des Kantons Solothurn (Projekt)

1. Ausgangslage

Die Verwaltung und die Gerichte des Kantons Solothurn bearbeiten täglich (besonders schützenswerte) Personendaten sowie sonstige sensible Informationen und betreiben Prozesse, von denen die Bevölkerung und teilweise auch Unternehmen direkt abhängig sind. Die Bedrohungslage durch Sicherheitsvorfälle und Datenpannen hat in den letzten Jahren deutlich zugenommen – nicht zuletzt aufgrund der rasant fortschreitenden Digitalisierung in sämtlichen Bereichen. E-Government-Dienste, digitale Aktenführung, Auslagerungen von Informatikdienstleistungen, vernetzte Fachanwendungen und mobile Arbeitsplätze erhöhen die Angriffsfläche und die Komplexität der zu schützenden Informationslandschaft erheblich. Jede neue Anwendung, jede Schnittstelle zu Dritten und jeder digitale Geschäftsprozess stellt ein potenzielles Sicherheitsrisiko dar. Ein Informationssicherheitsmanagementsystem (ISMS) ist das anerkannte Instrument, um diesen Herausforderungen systematisch und nachweisbar zu begegnen. Es stellt Regeln und Verfahren auf, um Informationssicherheit und Datenschutz[1] dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Zur Sicherstellung dieser Vorgaben werden angemessene technische und organisatorische Massnahmen umgesetzt.

Die kantonale Verwaltung und die Gerichte tragen eine besondere Verantwortung im Bereich Informationssicherheit und Datenschutz. Sie haben sicherzustellen, dass sie mit anerkannten Standards und mit der Entwicklung der Bedrohungslage Schritt halten, um die staatliche Leistungserbringung und das Vertrauen in den Staat bestmöglich zu gewährleisten. Dies dient nicht nur der Schadensvermeidung (finanzieller Schaden, Reputationsschaden, Beeinträchtigung kritischer Infrastrukturen), sondern besonders auch der Rechtskonformität bzw. dem Schutz von Personendaten der Bevölkerung. Fehlende kantonale Koordination kann zu Verletzungen von Informationssicherheit und Datenschutz führen und somit konkrete, öffentlichkeitswirksame Konsequenzen haben. Es sollte daher ein strukturierter, kantonal koordinierter Ansatz zum wirksamen Schutz von Informationen in der kantonalen Verwaltung und bei den Gerichten verfolgt werden. Informationssicherheit und Datenschutz sind im Gesamtkontext zu betrachten und mittels entsprechender Führungs- und Steuerungsinstrumente aktiv zu behandeln.

Der Regierungsrat hat mit RRB Nr. 2019/823 vom 21. Mai 2019 die Leitlinie Informationssicherheit der kantonalen Verwaltung Solothurn sowie mit RRB Nr. 2020/1659 vom 24. November 2020 das Konzept Informationssicherheit der kantonalen Verwaltung verabschiedet. Mit RRB Nr. 2026/800 vom 28. April 2026 wurden diese sodann an aktuelle Gegebenheiten angepasst. Diese beiden Dokumente bilden eine erste Grundlage im Bereich Informationssicherheit.

---

[1] Datenschutz bezeichnet den Schutz der Persönlichkeit und der Grundrechte von Personen bei der Bearbeitung ihrer Personendaten. Informationssicherheit geht weiter und umfasst den Schutz sämtlicher Informationen – unabhängig davon, ob es sich um Personendaten handelt oder nicht – hinsichtlich ihrer Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit. Der Datenschutz versteht sich im vorliegenden Kontext daher als Teil der Informationssicherheit.

Das Amt für Informatik und Organisation (AIO) ist ISO/IEC 27001[2] zertifiziert. Diese Zertifizierung belegt, dass das AIO als IKT-Leistungserbringer für den Kanton ein strukturiertes ISMS für seinen eigenen Leistungsbereich betreibt. Daraus folgt jedoch ausdrücklich nicht, dass die übrigen kantonalen Dienststellen damit von der Verantwortung entbunden sind, ihrerseits die Informationssicherheit systematisch zu managen. Informationssicherheit beschränkt sich nicht auf die IKT-Infrastruktur. Sie betrifft ebenso beispielsweise organisatorische Abläufe, Papierakten, die Sicherheitskultur der Mitarbeitenden, den Umgang mit externen Dienstleistern, Zutrittskontrollen, Klassifizierung bzw. Einstufung von Informationen und das Risikomanagement der Fachgeschäftsprozesse und -anwendungen. Damit liegt ein erheblicher Teil der Verantwortung bei den Dienststellen selbst – unabhängig davon, welche IKT-Dienstleistungen das AIO erbringt. Dieses ist ein wichtiger Kooperationspartner und insbesondere technischer Leistungserbringer. Die inhaltliche Verantwortung für Informationssicherheit und Datenschutz des Geschäftsbetriebs verbleibt jedoch direkt bei den Dienststellen. Aktuell werden diese Themen in den Dienststellen hingegen sehr unterschiedlich umgesetzt.

2. Situation auf Bundesebene und Auswirkungen auf die Kantone

Der Bund hat in den vergangenen Jahren den regulatorischen Rahmen im Bereich der Informationssicherheit substanziell ausgebaut. Das Informationssicherheitsgesetz (ISG, SR 128) schafft einen einheitlichen Rahmen für die Informationssicherheit beim Bund. Es legt den Fokus auf die kritischsten Informationen und Systeme sowie auf die Standardisierung der Massnahmen. Somit soll die Informationssicherheit beim Bund nachhaltig und wirtschaftlich verbessert werden.[3] Die Informationssicherheitsverordnung (ISV, SR 128.1) verpflichtet sodann gewisse Verwaltungseinheiten[4] zur Einführung eines ISMS und referenziert dabei auf die oberste Führungsverantwortung (Art. 5 ISV i.V.m. Art. 7 Abs. 1 ISG[5]). Das ISG kommt für die Kantone nur bedingt zur Anwendung. Gemäss Art. 3 Abs. 1 gelten für die Kantone die Bestimmungen über klassifizierte Informationen (Art. 11 ff.), soweit sie klassifizierte Informationen des Bundes bearbeiten. Weiter gelten die Bestimmungen über die Sicherheit beim Einsatz von Informatikmitteln[6] (Art. 16 ff.), soweit die Kantone auf Informatikmittel des Bundes zugreifen. Diese Bestimmungen gelten hingegen nicht, wenn die Kantone eine mindestens gleichwertige Informationssicherheit gewährleisten (Art. 3 Abs. 2 als subsidiäre Auffangnorm). Sie müssen entsprechend sicherstellen, dass ihre Massnahmen tatsächlich geeignet dafür sind, das erforderliche Sicherheitsniveau zu erreichen. Der Umfang dieser Prüfung ist auf die Sicherheit bei der Bearbeitung von klassifizierten Informationen und beim Zugriff auf Informatikmittel des Bundes beschränkt. Für diese Kontrolle sind die Kantone selbst zuständig.[7]

Die weiterentwickelte Nationale Cyberstrategie (NCS) wurde im April 2023 sowohl durch den Bundesrat als auch via KKJPD (Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren) durch die Kantone gutgeheissen. Die Strategie zeigt auf, mit welchen Zielen und Massnahmen der Bund und die Kantone gemeinsam mit der Wirtschaft und den Hochschulen den Cyberbedrohungen begegnen wollen.[8] Die Kantone definieren ihre Organisation der Cyber-

---

[2] Hinter der Abkürzung ISO steht die Internationale Organisation für Normung bzw. Standardisierung. Die ISO entwickelt in verschiedenen Bereichen weltweit gültige Standardnormen. Für Themen, die mit Elektrik und Elektronik zu tun haben, haben sich die IEC-Normen der «International Electrotechnical Commission» durchgesetzt. ISO/IEC 27001 ist der angewendete Standard für die Zertifizierung eines ISMS.

[3] BBl 2017 2953, S. 2954

[4] Bundeskanzlei, Generalsekretariate, Gruppen und Bundesämter

[5] Art. 7 Abs. 1 ISG: «Die verpflichteten Behörden sorgen in ihrem Zuständigkeitsbereich dafür, dass die Informationssicherheit nach dem Stand von Wissenschaft und Technik organisiert, umgesetzt und überprüft wird.»

[6] Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen (Art. 5 Bst. a ISG).

[7] BBl 2017 2953, S. 3070

[8] Der Bundesrat und die Kantone legen die neue Nationale Cyberstrategie fest, 13.04.2023, https://www.news.admin.ch/de/nsb?id=94237

sicherheit selbständig und angepasst an ihren Bedarf. Sie sind verantwortlich für den Schutz ihrer Dienstleistungen und müssen bei der Erfüllung ihres Auftrags eine hohe Verfügbarkeit aufweisen.[9]

Die Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) wurde sodann im Juni 2023 aktualisiert. Der Schutz der kritischen Infrastrukturen vor Cyberrisiken stellt einen wesentlichen Bestandteil der NCS dar. Die NCS und die SKI-Strategie sind eng aufeinander abgestimmt.[10] In der SKI-Strategie sind acht Massnahmen definiert, mit denen der Bundesrat die Versorgungssicherheit in der Schweiz erhalten und in wesentlichen Bereichen verbessern will. Verschiedene Massnahmen betreffen auch die Kantone unmittelbar. Sie führen SKI-Arbeiten im Rahmen ihrer Kompetenzen und Aufgaben sowie entsprechend ihren Möglichkeiten und Bedürfnissen durch.[11] Gemäss SKI-Strategie zählen «Behörden» (Teilsektor «Parlament, Regierung, Justiz, Verwaltung») zu den kritischen Infrastrukturen mit grosser Kritikalität.[12] Aus SKI-Perspektive besonders relevante Leistungen sind (nicht abschliessend) Gesetzgebung, Lenkung und Vollzug der Staatsaufgaben, Rechtsprechung und -vollzug sowie allgemeine Verwaltungsaufgaben (u. a. Warnung und Alarmierung bei Gefahr, Wahrung der inneren Sicherheit).[13]

3. Rechtsgrundlage

Die Rechtsgrundlage für ein kantonal übergeordnetes ISMS ist gestützt auf § 25 Abs. 2 Bst. b WoV-G gegeben, denn ein ISMS zählt zu zeitgemässen Führungs- und Organisationsinstrumenten.

Gemäss Art. 71 Abs. 1 KV erlässt der Kantonsrat alle grundlegenden und wichtigen Bestimmungen in Form des Gesetzes. Angesichts der wachsenden Bedeutung der Informationssicherheit, der fortschreitenden Digitalisierung und der damit verbundenen Risiken sollte die Informationssicherheit als öffentliche Aufgabe ausdrücklich gesetzlich normiert werden. Die entsprechende Überprüfung hat im Rahmen zukünftiger Gesetzesänderungen oder beim Erlass neuer Gesetze zu erfolgen.

4. Ziel, Auftrag und Geltungsbereich

Informationssicherheit und Datenschutz sind Aufgaben des Kantons und liegen in der Verantwortung der obersten Führungsebene (Regierungsrat und Gerichtsverwaltungskommission). Ein kantonal übergeordnetes ISMS hat zum Ziel, diese Themen systematisch zu steuern. Es stellt sicher, dass sie definiert, kontrolliert, aufrechterhalten und fortlaufend verbessert werden. Die oberste Führungsebene gewährleistet damit eine nachweisbare und wirksame Wahrnehmung ihrer Verantwortung.

Da es sich um ein transversales Vorhaben handelt, ist eine Arbeitsgruppe ISMS (AG ISMS) mit Vertreterinnen und Vertretern sämtlicher Departemente, der Staatskanzlei, der Gerichte, des AIO sowie der Beauftragten für Information und Datenschutz (IDSB) einzusetzen. Die Arbeitsgruppe hat zum Auftrag, unter Berücksichtigung der Rahmenbedingungen, ein kantonal übergeordnetes ISMS strukturiert und koordiniert aufzubauen. Die HERMES-Projektmethodik des Kantons kommt analog zur Anwendung. Mit Abschluss des Projekts (geplant im Q1 2029) ist das ISMS in den regulären Betrieb zu überführen. Hierzu werden dem Regierungsrat und der Gerichtsverwaltungskommission die erforderlichen Grundlagendokumente, die während des Projekts ausgearbeitet werden, zum Beschluss unterbreitet.

---

[9] NCS 2023, S. 10 und 12
[10] SKI vom 16.06.2023, S. 5
[11] SKI vom 16.06.2023, S. 3 f.
[12] SKI vom 16.06.2023, S. 7
[13] SKI vom 16.06.2023, S. 25

Das kantonal übergeordnete ISMS gilt für alle Behörden der kantonalen Verwaltung, inkl. den Gerichten. Nicht unter den Geltungsbereich fallen – analog Digitalisierungs- und IKT-Strategie – die Solothurner Spitäler AG, die Fachhochschule Nordwestschweiz, die selbständigen öffentlich-rechtlichen Anstalten des Kantons und der Informatik-Einsatz in den kantonalen Schulen für Unterrichtszwecke.

Für die Gerichte erlangt der Inhalt des vorliegenden Regierungsratsbeschlusses erst nach entsprechendem Gerichtsverwaltungskommissionsbeschluss Verbindlichkeit.

5. Verantwortlichkeiten, Zuständigkeiten und Schnittstellen

Die Gesamtverantwortung für die Informationssicherheit und den Datenschutz liegt bei der obersten Führungsebene (Regierungsrat und Gerichtsverwaltungskommission), welche verbindliche Vorgaben erlässt. Zur Sicherstellung einer einheitlichen Vorgehensweise und methodischen Konsistenz übernimmt die AG ISMS die strategischen Arbeiten sowie die Koordination im Rahmen des Projekts. Sie erarbeitet Vorgaben zu Methoden, Prozessen, Standards etc. Die Verantwortung zur Umsetzung obliegt den einzelnen Departementen, Ämtern bzw. Dienststellen und Gerichten. Damit die ISMS-Vorgaben wirksam umgesetzt werden können, ist ein koordiniertes Zusammenwirken aller Beteiligten erforderlich.

Weiter ist eine enge Abstimmung insbesondere mit dem Integrierten Risikomanagement (IRM)[14] und dem Internen Kontrollsystem (IKS, § 41 Verordnung zum Gesetz über die wirkungsorientierte Verwaltungsführung) sicherzustellen, um Überschneidungen zu vermeiden, Schnittstellen effizient zu gestalten und Synergien optimal zu nutzen.

6. Finanzierung von Externen

Das Finanzdepartement trägt die Kosten für den Beizug externer Expertinnen und Experten in der Initialisierungsphase. Für die weiteren Projektphasen ist die Kostenverteilung dem Regierungsrat zum Beschluss zu unterbreiten. Er legt den Verteilschlüssel fest.

Den Gerichten auferlegte Kosten erlangen erst nach entsprechendem Gerichtsverwaltungskommissionsbeschluss Verbindlichkeit.

7. Nutzen

Ein kantonal übergeordnetes ISMS bringt insbesondere in folgenden Bereichen einen wesentlichen Nutzen:

- Rechtssicherheit und Compliance: Berücksichtigung rechtlicher Grundlagen, übergeordneter Strategien und Angleichung an den Bund, Einhaltung von kantonalen Strategien und Vorgaben, Berücksichtigung von anerkannten Normen und Standards bzw. des aktuellen Stands der Praxis (sog. «Best Practices»)

- Einheitlichkeit: kantonal einheitlicher Standard und Einbettung in übergeordnete Steuerungsarchitektur

- Synergienutzung: effiziente Nutzung bestehender Ressourcen und Strukturen

- Vertrauensbildung: Stärkung des internen und externen Vertrauens

[14] RRB Nr. 2025/1705 vom 21. Oktober 2025

- Vermeidung von und Umgang mit Sicherheitsvorfällen: Sicherheitsvorfälle und Datenpannen weitmöglichst vermeiden bzw. erkennen und Lehren daraus ziehen

8. Beschluss

8.1 Das Projekt «Informationssicherheitsmanagementsystem (ISMS) der Verwaltung und der Gerichte des Kantons Solothurn» wird freigegeben und analog der HERMES-Projektmethodik des Kantons durchgeführt (Abschluss geplant im Q1 2029).

8.2 Im Rahmen des Projekts werden die erforderlichen Grundlagendokumente zur Überführung des ISMS in den regulären Betrieb ausgearbeitet und dem Regierungsrat zum Beschluss unterbreitet.

8.3 Für das Vorhaben wird eine Arbeitsgruppe (AG ISMS) unter der Leitung des Finanzdepartements mit folgenden Mitgliedern eingesetzt:

- Informationssicherheitsverantwortliche der Departemente, der Staatskanzlei und der Gerichte
- Vertretung des AIO
- Beauftragte/r für Information und Datenschutz (IDSB), beratend (ohne Stimm- und Antragsrecht)

Die Mitglieder haben über Kenntnisse in mindestens einem der folgenden Bereiche zu verfügen: Informationssicherheit, Datenschutz, IKT oder Risikomanagement. Sie sind bis zum 30. Oktober 2026 zu benennen und der Arbeitsgruppenleitung mitzuteilen.

8.4 Die Koordinationskommission (KoKo) wird als Steuerungsausschuss eingesetzt.

8.5 Die AG ISMS kann weitere Personen, insbesondere aus der kantonalen Verwaltung und den Gerichten, zu den Arbeiten beiziehen. Diese Personen haben weder Stimm- noch Antragsrecht.

Yves Derendinger
Staatsschreiber

Beilage

Projektauftrag «Informationssicherheitsmanagementsystem (ISMS) der Verwaltung und der Gerichte des Kantons Solothurn»

Verteiler

Departemente (5)
Staatskanzlei
Gerichtsverwaltung
Mitglieder der AG ISMS (elektronischer Versand durch Finanzdepartement)