KANTON AARGAU

DEPARTEMENT
FINANZEN UND RESSOURCEN
Informatik Aargau

Informationssicherheit

24. Juni 2025

FACT SHEET

Geplantes kantonales Informationssicherheitsgesetz (InfoSiG) / Informationssicherheit in den Aargauer Gemeinden

1. Ausgangslage

Der Verband der Aargauer Gemeindeschreiberinnen und Gemeindeschreiber (AAG), der Verband Finanzfachleute Aargauer Gemeinden (FAG) sowie der Fachverband ICT Verantwortliche Aargauer Gemeinden (VIA) haben im Austausch mit der kantonalen Verwaltung im Rahmen der Anhörung zum kantonalen Informationssicherheitsgesetz (InfoSiG) den Wunsch nach Unterstützung geäussert. Zum einen wünschen sie mit Blick auf die Budgetrunde für das Jahr 2026 Anhaltspunkte zur Einordnung der Aufwände bezüglich des InfoSiG zu erhalten. Zum anderen bitten sie um Unterstützung bei der Umsetzung der Informationssicherheit, insbesondere für kleinere Gemeinden ohne eigene ICT-Fachpersonen.

In den vergangenen Jahren haben die Risiken im Bereich der Informationssicherheit und dem Datenschutz in der Verwaltung (Bund, Kantone, Gemeinden) stark zugenommen. Zwar schafft der vermehrte Einsatz von vernetzten Informatikmitteln Effizienzen, bietet jedoch Cyber-Kriminellen die Möglichkeit, Schwachstellen in Systemen auszunutzen.

Der Bund hat mit dem Inkrafttreten des Informationssicherheitsgesetz (ISG) am 1. Januar 2024 seinen eigenen Schutz definiert und mittels Nationaler Cyber Strategie (NCS) das Erfordernis einer digitalen Resilienz für die kritische Infrastrukturen[1] vorgegeben. Öffentliche Verwaltungen sind ein Teil dieser kritischen Infrastrukturen.

Der Kanton Aargau wird seinerseits mit der Inkraftsetzung des kantonalen Gesetzes über die Informationssicherheit (InfoSiG) voraussichtlich per 1. Juli 2026 im Bereich der Cybersicherheit gesetzgeberisch tätig. Das Gesetz soll die Informationssicherheit gesetzlich verankern und regelt den Schutz von Informationen, IT-Systemen und Infrastrukturen gegen Missbrauch, Ausfälle und Angriffe – insbesondere im Kontext der zunehmenden Digitalisierung und Cyberbedrohungen. Damit verbessert der Kanton Aargau seine Position gegen die zunehmende Bedrohung aus dem Cyberraum.

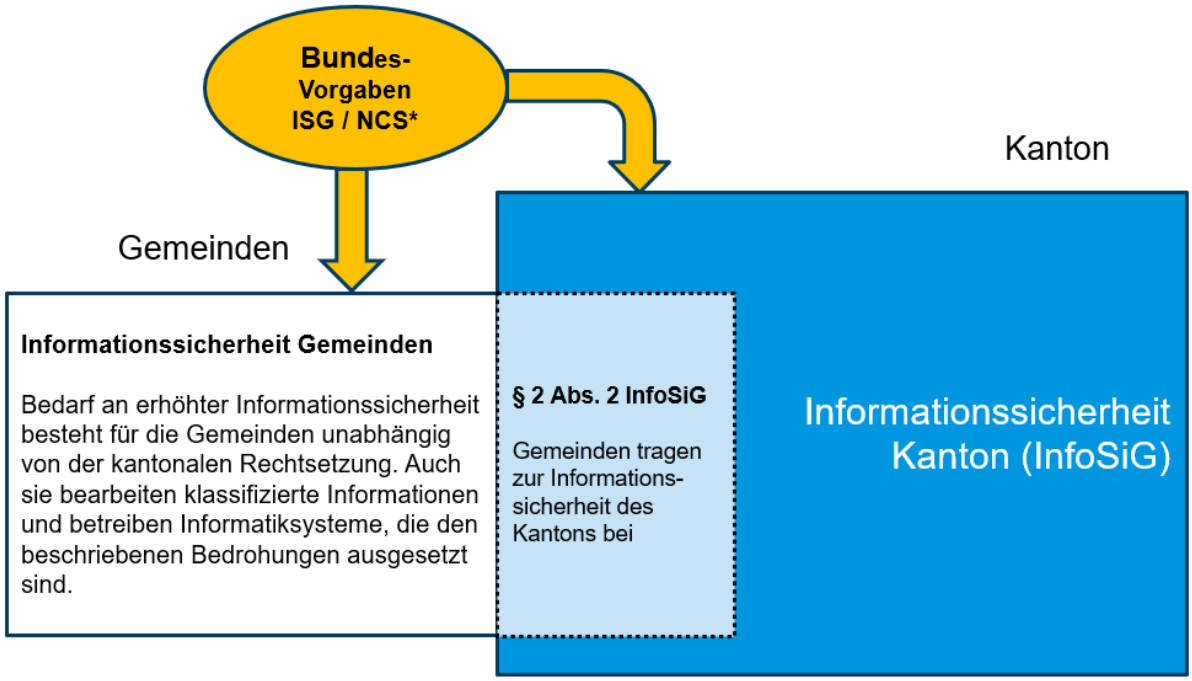
OBJ Was bedeutet die Einführung des InfoSiG für die Aargauer Gemeinden konkret?

Mit dem kantonalen Informationssicherheitsgesetz sollen Grundlagen zum Eigenschutz aus dem digitalen Raum geschaffen werden. Ebenfalls wird das Schutzniveau von externen Zugriffen auf Datenbestände der Verwaltung geregelt. In diesem Zusammenhang werden auch die Gemeinden neu in §2 Abs 2 InfoSiG adressiert und zur Einhaltung eines bestimmten Schutzniveaus verpflichtet

[1] Kritische Infrastrukturen: https://www.babs.admin.ch/de/die-kritischen-infrastrukturen

(siehe Abbildung 1). Als Richtschnur für das Schutzniveau wird zum Beispiel der vom Bundesamt für wirtschaftliche Landesversorgung herausgegebene IKT-Minimalstandard[2] herangezogen.

Abbildung 1: Cybersicherheit Bund, Kanton, Gemeinden



*ISG: Bundesgesetz über die Informationssicherheit beim Bund / (Informationssicherheitsgesetz, ISG)
NCS: Nationale Cyberstrategie

1.1 Geltungsbereich des kantonalen Gesetzes für Gemeinden

§2 Abs 2 InfoSiG beschreibt den Geltungsbereich. Das neue kantonale Gesetz gilt grundsätzlich für Gemeinden, wenn diese

- klassifizierte Informationen des Kantons bearbeiten (z. B. vertrauliche Daten aus kantonalen Systemen)
- auf kantonale Informatikmittel zugreifen

Es soll keine Anwendung finden, wenn ein mindestens gleichwertiger Sicherheitsstandard wie derjenige der kantonalen Verwaltung gewährleistet ist. Dabei gilt der IKT-Minimalstandard als Richtschnur.

Unabhängig davon, ob eine Gemeindetätigkeit in den Geltungsbereich von §2 Abs. 2 InfoSiG fällt, sind *Massnahmen zur Stärkung der Cyber-Resilienz* aufgrund enger Vernetzung von Informatiksystemen, der Vorgaben zur nationalen Cyberstrategie, den Anforderungen an die kritische Infrastruktur (Grundversorgung, Schulen, Verwaltungen, etc.) sowie der mannigfachen Bedrohungen aus dem Cyberraum[3], *dringend empfohlen*.

1.2 Selbstorganisation der Gemeinden

In der Anhörung zum InfoSiG wurde durch den Kanton kommuniziert, dass dieser **keine Schutzverantwortung** für die IT-Systeme der Gemeinden übernimmt und keine **finanzielle oder operative Unterstützung** vorsieht, um die Gemeindeautonomie und die Wettbewerbsneutralität zu wahren.

[2] IKT-Minimalstandards: https://www.bwl.admin.ch/de/ikt-minimalstandards - seit 2025 beim BACS: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html
[3] Cyberrisiken seit Jahren auf Platz 1 - Allianz Risk Barometer 2025: https://www.allianz.ch/de/ueber-uns/medien/medienmitteilungen-presse-kit/2025/allianz-risk-barometer.html

Gemeinden sollen sich **selbst organisieren**, zum Beispiel durch Kooperationen, durch Verbund oder internen Austausch.

1.3 Punktuelle Unterstützung durch den Kanton

Bei Annahme des InfoSiG wird eine kantonale Cyber-Koordinationsstelle geschaffen, die auch Gemeinden als eine zentrale Anlaufstelle für Fragen zur Informationssicherheit zur Verfügung stehen wird. Sie bietet Beratungen, Schulungen, Sensibilisierung und Koordination, aber keine operative Unterstützung.
Der Kanton hat ein grosses Interesse an der Resilienz der gesamten Verwaltung und bietet bis zur Einführung der Cyberkoordinationsstelle punktuelle Unterstützung durch den Chief Information Security Officer (CISO) für Seminare, Info-Veranstaltungen und Referate.

2. Handlungsbedarf

Die allgemeine Bedrohungslage, das Informationssicherheitgesetz des Bundes (ISG), die Nationalen Cyberstrategie (NCS) sowie das geplante kantonale InfoSiG, zur Sicherstellung eines minimalen Standards, sind mit Herausforderungen verbunden. Jetzt ist der richtige Zeitpunkt für Gemeinden – unabhängig von der Inkraftsetzung des kantonalen Gesetzes – sich strategisch gegen Cyberbedrohungen zu schützen. Folgende Prioritäten werden durch den CISO empfohlen:

2.1 Leitungsebene

- grundsätzliches Sicherheitsbewusstsein etablieren.
- Geschäftsleitung der Gemeinde prüft Bedrohungslage durch Cyberrisiken auf eigene Prozesse regelmässig. Insbesondere folgende Themen sind zu adressieren (Beispiele):
  - Datenverlust (Verschlüsselung, unautorisierte Bekanntgabe, Erpressung)
  - Betriebsunterbrechung (Schutz des Backups, Wiederherstellung, Notfallprozesse)
  - Kompromittierung (Infiltration durch Malware, unautorisierter Zugriff von innen oder aussen, Lieferantensicherheit, physische Sicherheit)
- Aufgaben, Kompetenzen und Verantwortlichkeiten klären
- Mitarbeitende bezüglich Informationssicherheits- und Datenschutzrisiken schulen. Schulung von Mitarbeitenden zu Themen wie Phishing, Passwortsicherheit, Umgang mit vertraulichen Daten[4].

2.2 ICT-Umgebung

- GAP-Analyse: Ist Minimalstandard[5] bereits erfüllt oder gibt es Entwicklungspotential?
- Externe und/oder interne Dienstleister sind informiert und sich der Aufgaben und Schritte bewusst, welche zur Entwicklung einer höheren Cyber-Resilienz führen und wie z.B. der IKT-Minimalstandard des Bundes erreicht werden kann.

[4] Zum Beispiel via https://elearningcyber.ch/ , Kurse, Austausch, etc.

[5] Mindeststandard: Standards dienen einem gemeinsamen Verständnis. Gemeinden müssen einen Minimalstandard erfüllen, um vom kantonalen Gesetz ausgenommen zu sein. Als Massstab kann der IKT-Minimalstandard oder die ISO Norm 27001 zur Orientierung herangezogen werden. Diese Standards definiert grundlegende Anforderungen an Informationssicherheit (z. B. Zugriffsschutz, Verschlüsselung, Risikomanagement).
Der IKT-Minimalstandard des Bundes steht voraussichtlich Ende 2025 in einer vereinfachten Version zu Verfügung.
Es dürfen auch weitere Normen, Hilfsmittel oder Strategien zur Erfüllung einer fundierten Cybersicherheit benutzt werden. Beispiele: https://cybernavi.ch/ , https://www.s-u-p-e-r.ch/de/machen/ , https://www.cyber-safe.ch/

- Investitionen in IT-Sicherheit (technisch) werden in die Planung aufgenommen. Dies kann in den meisten Fällen im normalen Lifecycle eines Produktes mitaufgenommen werden.
- Pflichten bezüglich Sicherheit sind Lieferanten vertraglich zu übertragen[6].

2.3 Kooperationen

- IT-Dienstleister haben oft mehrere Kunden aus der gleichen Branche. Die Zusammenarbeit mehrerer Gemeinden mit ihren jeweiligen Dienstleister schafft Effizienzen.
- Häufige Ursachen von Cybersicherheitsvorfällen sind auch bei Lieferanten zu verorten. Bei Beschaffungen von Lieferanten wie auch Zugriffen durch Lieferanten sind auf aktuelle Sicherheitsstandards zu achten. Die meisten Lieferanten sind sich den Themen bewusst und unterstützen das gemeinsame Ziel, besser zu werden. Eine offene Sicherheitskultur ist wichtig. Eine gemeinsame Table-Desk Notfall-Übung bezieht beide Parteien mit ein.

2.4 Budgetierung

Aufgrund der verschiedenen Reifegrade und der technologischen sowie organisatorischen Unterschiede ist es schwierig, eine Aussage über direkte oder indirekte Investitionen und wiederkehrende Kosten tätigen zu können. Nachfolgend eine empfohlene Priorisierung von Themen:

- Einplanen Gap-Analyse. Bei externer Vergabe mit Lieferanten oder spezialisierter Firma ab circa Fr. 3'000.– (https://www.cyber-safe.ch/) bis über Fr. 12'000.–.
- Ausbildung interner Mitarbeitenden.
  - https://elearningcyber.ch/ [7] Fr. 0.– (vom Bund zur Verfügung gestellt)
  - externe Firmen bieten Seminare vor Ort oder Remote ab circa Fr. 1'500.– / Tag. Kooperationen unter Gemeinden lohnen sich.
- Technische Aspekte (zu priorisieren)
  - Multi-Faktor-Authentifizierung (MFA): Mit einer Multi-Faktor-Authentifizierung werden privilegierte Zugänge und externe Zugänge generell mit einem zweiten Faktor abgesichert. Offerte eines Dienstleisters. Microsoft, Cisco DUO oder weitere Anbieter prüfen.
  - Backup: Falls die Infrastruktur komplett verschlüsselt wird, muss der Zugriff auf ein unverschlüsseltes, funktionierendes Backup trotzdem noch möglich sein. Neben der Sicherheit gegen eine Verschlüsslelung muss auch die Wiederherstellung regelmässig getestet werden.
  - Virenschutz: Ein effizienter und effektiver Virenschutz stellt sicher, dass frühzeitig Gefahren erkennt werden können. Es sollte sich dabei um ein Produkt mit automatischen Isolationsmöglichkeiten und Alarmierungsoptionen[8] handeln. Mit dem Anbieter muss vereinbart sein, ob die Reaktion auf Virenschutz-Alarme und Kompromitierung manuell oder primär automatisiert reagiert werden soll.

[6] Vertragliche Verpflichtungen: Informationssicherheit betrifft insbesondere auch Drittanbieter, die im Auftrag der Gemeinde arbeiten. Insbesondere Lieferanten im Bereich ihrer ICT-Infrastruktur und sollte vertraglich geregelt werden.
[7] In der Plattform können auch Teams gebildet werden. Somit können die Schulungsergebnisse zentral nachgewiesen / aufbewahrt werden.
[8] EDR / XDR Systeme für Virenschutz einsetzen. Ein EDR (Endpoint Detection and Response) ist ein Sicherheitssystem, das Endgeräte wie PCs überwacht, Bedrohungen erkennt und darauf reagiert. XDR (Extended Detection and Response) geht weiter: Es integriert Daten aus mehreren Quellen (z. B. Endpunkte, Netzwerke, Server, Cloud), um Bedrohungen umfassender zu erkennen und zu bekämpfen. Beide Systeme verbessern die IT-Sicherheit durch frühzeitige Erkennung und automatisierte Reaktionen.

Grundsätzliche Massnahmen zu fehlenden Sicherheitsmassnahmen infolge der Resultate der internen oder externen Gap-Analyse sollten über den Zeitraum von Lebenszyklen und Re-Investitionen eingeplant werden. Dringliche Massnahmen (siehe "technische Aspekte") sind zu priorisieren, falls nicht vorhanden.

David Schlaginhaufen
CISO Kanton Aargau

Anhänge:

- Tabellen Minimalstandard
- Tabelle Mindestanforderungen Authentifizierung
- Tabelle Minimal-Checkliste zur Cyberresilienz für kleinere Gemeinden

3. Anhang

3.1 Orientierung IKT – Minimalstandard

Die nachfolgenden Handlungsfelder sind ein Zusammenzug aus dem IKT-Minimalstandard des Bundes und enthalten die wesentlichen Themenbereiche zum Ausbau der Resilienz gegenüber Cyberbedrohungen.

- Die Anforderungen sollten im Grundsatz erfüllt werden.
- Die möglichen Massnahmen zu technischen und organisatorischen Aspekten (TOM) sind je nach Grösse, Reifegrad, Risikoassessment in den Gemeinden unterschiedlich ausgeprägt.
- Die Verantwortlichkeiten für die Themen sind als Vorschlag in Geschäftsleitung / Gemeinderat (GL) und interner / externer IT-Dienstleister (IT) aufgeteilt.

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
Governance / Steuerung	Sicherheitsorganisation	Die Sicherheitsorganisation muss definiert und gegenüber den Mitarbeitenden kommuniziert sein bzw. in dieser Form auch gelebt werden. Kontaktpersonen mit ihren Zuständigkeiten und Verantwortlichkeiten für die strategische und operative Cybersicherheit nachvollziehbar festgelegt. Fachliche Befähigung dieser Personen	• GL übernimmt Verantwortung • definiert Person(en) zur Umsetzung (oder/und lässt durch IT/Security Dienstleister in Auftrag beraten und umsetzen) • Kommuniziert die Sicherheitsorganisation an Mitarbeitende	X	
Governance / Steuerung	Cyberrisikomanagement	Cyberrisikomanagement muss definiert und festgelegt sein, d. h. es muss geklärt sein, ob und wie mit Cyberrisiken umzugehen ist, und wie die Geschäftsleitung eingebunden ist. Für die Beurteilung und Einstufung von Cyberrisiken (z. B. sicherheitsrelevante Vorfälle) müssen Kriterien definiert sein, und für kritische Cyberrisiken müssen adä-	• GL nimmt Risiken z.B. in IKS auf, oder definiert eigenes Cyber-Risiko Management • GL definiert Massnahmen, eine Liste / Checkliste / Umsetzungsplan mit techn. und organ. Massnahmen • Ausfallzeiten, Wiederanlaufzeiten sind definiert • Reaktion, Meldewege bei Datenverlust, Erpressung oder ähnlichen Vorfällen ist definiert (KAPO, Bund, Kanton, OEDB) https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-behoerden/vorfall-was-nun.html • TOMs: https://cybernavi.ch/#start / https://www.s-u-p-e-r.ch / https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html	X	

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
		quate TOMs (technische und organisatorische Massnahmen) bestimmt und umgesetzt sein.			
Governance / Steuerung	Überprüfung MA / DL	Vertrauenswürdigkeit Mitarbeitende und Dienstleister gemäss Verantwortungsebenen und Tätigkeiten überprüfen.	• Hintergrunds-Überprüfung stufengerecht • Minimum Strafregister & Betreibungsregisterauszug • Periodische Überprüfung	X	
Governance / Steuerung	Schulung und Sensibilisierung	Mitarbeitende müssen im Hinblick auf Fragen der Cybersicherheit ihren Stufen und Tätigkeiten entsprechend sensibilisiert und geschult sein. Im Rahmen der Schulungen müssen soweit möglich tatsächliche Vorfälle und daraus resultierende Schlussfolgerungen für die Organisation oder das Unternehmen thematisiert werden.	• Schulungsangebote Dienstleister evaluieren / periodische Schulungen, z.B. mit ext. Referenten • https://www.elearningcyber.ch/ dort können Teams gebildet werden • Material KAPO: https://www.ag.ch/de/verwaltung/dvi/kantonspolizei/praevention/cybercrime#MjIzNDIwNA	X	
Identifizieren / Identify	Informatikschutzojekte (ISDS-Konzept)	Alle (wesentlichen) Hard- und Softwarekomponenten, Serverräume, der IT-Infrastruktur müssen im Hinblick auf ihren Schutzbedarf analysiert sein. Logisch zusammengehörende Komponenten zusammenfassen und zu einem Informatikschutzobjekt aggregieren. Die entsprechenden Dokumentationen müssen alle umgesetzten oder noch umzusetzenden TOMs mit umfassen und stets aktuell gehalten werden.	• Register mit Inventar, die "Kritikalität" / Schutzbedarf, dazu gehörende Risiken und vor allem Massnahmen der IT-Schutzobjekten auf die AspekteVERTRAULICHKEIT, VERFÜGBARKEIT, INTEGRITÄT • Mit Datenschutz Anforderungen ergänzen. Allenfalls im gleichen Register die Datenbestände / Kategorien mitführen • kann zusammen mit IT-Dienstleister erstellt werden • Bei Vertraulichkeit u.U. Klassifizierungen einführen	X	

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
Identifizieren / Identify	Lieferkettenmanagement	Alle Abhängigkeiten in den IT-Lieferketten müssen identifiziert, ihre Bedeutung / Kritikalität für die Geschäftstätigkeit (d. h. die Geschäfts- und Produktionsprozesse) beurteilt und überwacht werden. Insbesondere muss sichergestellt sein, dass die Lieferanten von für die Geschäfts- und Produktionsprozesse wesentlichen Hard- und Softwarekomponenten und IT-Dienstleistungen (z. B. SaaS-Dienstleistungen), sowie die Lieferanten mit privilegierten Zugriffsmöglichkeiten durch die Umsetzung von adäquaten TOMs selbst auch bestmöglich abgesichert und damit resilient sind.	• Überprüfung und Absicherung Zugriff externer Lieferanten • Nur persönliche Accounts bei Lieferanten • Accounts extern immer mit zweitem Faktor abgesichert • Kontaktliste / Notfallkontakte • Vertragliche SLA für schnelle Reaktionszeit im Notfall und bei Schwachstellen, zeitnahes "Patchen" / innerhalb von Stunden u.U. • Lieferant hat sein eigenes Sicherheitsmanagement / Sicherheitszertifizierung • Nur verschlüsselte Datenübertragung		X

Schützen / Protect	Konfiguration und Betrieb	Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss so konfiguriert sein und betrieben werden, dass seine Angriffsfläche möglichst klein gehalten werden kann. Insbesondere müssen
		(a) ein adäquater physischer Schutz gegeben,
		(b) eine bestmögliche logische Abschottung und Isolierung
		(c) eine technische Härtung vorgenommen worden sein.
			• Physischer Schutz Ziel: Schutz vor unbefugtem physischen Zugriff
			  • Zutrittskontrollsysteme (Schloss, Kartenleser, Biometrie, etc.)
			  • Videoüberwachung / Alarmanlagen in Serverräumen
			  • Zugang nur für autorisiertes Personal (Need-to-know-Prinzip)
			  • Gehäuseschlösser für Endgeräte und Netzwerkkomponenten
			  • Dokumentation und Protokollierung aller physischen Zugriffe
			• Logische Abschottung & Isolierung: Begrenzung der Kommunikationswege und Zugriff
			  • Netzwerksegmentierung (z. B. VLANs, DMZs) / Mikrosegmentierung in RZ
			  • Trennung von Diensten
			  • Firewall-Regeln und Access Control Lists (ACLs) zur Minimierung der Verbindungen
			  • Trennung von Entwicklungs-, Test- und Produktionsumgebungen
			• Technische Härtung: Minimierung potenzieller Schwachstellen durch gezielte Konfiguration
			  • Entfernung vordefinierter Konten
			  • Deaktivierung oder Löschung von Standard-Accounts (z. B. „admin“, „guest“)
			  • Änderung von Standardpasswörtern
			  • Deaktivierung nicht benötigter Dienste:
			  • Nur notwendige Dienste aktivieren (Prinzip der minimalen Funktionalität)
			• Regelmässige Überprüfung laufender Prozesse und Dienste
					X

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
Schützen / Protect	Schwachstellen Management	Jede IT-Komponente muss im Hinblick auf bekannt gewordene Schwachstellen automatisiert überwacht werden und gemäss Anweisungen Hersteller gewartet und auf möglichst aktuellem Stand gehalten werden (z. B. durch zeitnahes Einspielen von Patches oder Auswechseln von Komponenten). Bei vernetzten Geräten muss (wenn technisch möglich) ein automatisierter Firmware-Update-Mechanismus vorhanden und standardmässig aktiviert sein.	• Automatisierte Firmware-Updates aktivieren, sofern vom Hersteller unterstützt • Geräte mit veralteter Firmware identifizieren und priorisieren • Automatisierte Schwachstellenüberwachung • Vulnerability Scanner einsetzen (z. B. Nessus, Qualys, OpenVAS) • regelmässige Scans aller IT-Komponenten (mind. monatlich oder bei Änderungen) • Risikobasierte Priorisierung der Schwachstellen (CVSS, Kritikalität, Exposition) • Rollback-Strategie für fehlerhafte Updates • Herstelleranweisungen regelmässig prüfen (z. B. über Mailinglisten, RSS-Feeds, CVE-Datenbanken) • Standardmässig aktivierte Update-Funktion bei neuen Geräten sicherstellen von Update-Status (z. B. via SNMP, API oder Management-Konsole) • Verantwortlichkeiten klar definieren (z. B. Patch-Owner pro Systemgruppe / Dienstleister) • Schulungen für Admins zu sicherem Patch- und Firmware-Management		X

Identifizieren / Identify	Identitäts- und Zugriffskontrollmanagement	Ein Informatikschutzobjekt muss in ein umfassendes Identitäts- und Zugriffskontrollmanagement-system eingebunden sein, das sicherstellt, dass Zugriffe nur authentifiziert und autorisiert erfolgen können.
		(a) Ein Zugriff ist authentifiziert, wenn die Identität der zugreifenden Entität definiert und mit Hilfe eines dem Schutzbedarf entsprechenden Authentifikationsverfahrens, -mittels oder -dienstes verifiziert worden ist.
		(b) Ein Zugriff ist autorisiert, wenn die Zugriffsrechte und Privilegien der zugreifenden Entität den Zugriff in dieser Form auch zulassen. Dabei muss die Vergabe von Zugriffsrechten und Privilegien möglichst minimal erfolgen («Least Privilege»-Prinzip).
			• Authentifizierung (a) – Identität verifizieren
			  • Technische Massnahmen:
			  • Multi-Faktor-Authentifizierung (MFA) für alle kritischen Systeme und privilegierten Konten
			  • Zentraler Identity Provider (IdP) wie Azure AD, EntraID, Keycloak oder Okta
			  • Starke Authentifizierungsverfahren je nach Schutzbedarf: Passwort + Token (z. B. TOTP, FIDO2), zertifikatsbasierte Authentifizierung, Biometrie (z. B. Fingerabdruck, Gesichtserkennung)
			  • Single Sign-On (SSO) mit Session-Timeouts und Re-Authentifizierung bei sensiblen Aktionen
			  • Organisatorische Massnahmen:
			  • Richtlinie für Passwortsicherheit (z. B. Länge, Komplexität, Rotation), norm. Account 12-14 Zeichen komplex, priv. ab 24 Zeichen random → Passwortless evaluieren.
			  • Schulung der Mitarbeitenden zu sicheren Authentifizierungsverfahren
			  • Verwaltung von Identitäten über den gesamten Lebenszyklus (Joiner-Mover-Leaver-Prozess)
			• Autorisierung (b) – Zugriff nur mit Berechtigung
			  • Technische Massnahmen:
			  • Rollenbasiertes Zugriffskontrollmodell (RBAC)
			  • Zentrale Rechteverwaltung mit regelmässiger Synchronisation
			  • Automatisierte Rezertifizierungsprozesse von priv. oder externen Accounts (z. B. vierteljährlich)
			  • Protokollierung aller Zugriffsentscheidungen (z. B. in SIEM-Systemen)
					X

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT

			• Organisatorische Massnahmen:
			  • Vergabe von Rechten nach dem Least-Privilege-Prinzip
			  • Vier-Augen-Prinzip bei der Vergabe von Admin-Rechten
			  • Dokumentation und Genehmigungspflicht für Sonderrechte
			  • Regelmässige Reviews von Berechtigungen durch Fachverantwortliche
			• Integration & Überwachung
			  • Alle Systeme müssen an ein zentrales IAM-System angebunden sein
			  • Monitoring von Anomalien im Zugriffsverhalten (z. B. ungewöhnliche Uhrzeiten, Geolokationen)
			  • Automatisierte Sperrung bei Verdacht auf Missbrauch
			  • Audit-Trails für alle sicherheitsrelevanten Aktionen		

Schützen / Protect	Netzwerksicherheit	Gegenüber netzwerkbasierten Angriffen schützen. Ein solcher Schutz kann grundsätzlich
		auf zwei unterschiedliche Arten erreicht werden:
		Entweder wird die Komponente oder das Informatikschutzobjekt in einem separaten Netzwerk (Segment) betrieben, das über einen geeigneten Perimeterschutz mit einer Beschränkung von Netzwerkdiensten, -protokollen und -ports verfügt (im Sinne einer Firewall) oder "ZeroTrust-Architektur".
			• Technische Massnahmen:
			  • Netzwerksegmentierung: Trennung von Zonen (z. B. DMZ, interne Netze, Produktionsnetze)
			  • Einsatz von VLANs oder physischen Trennungen
			  • Firewall-Regeln: Whitelisting von erlaubten Protokollen, Ports und IP-Adressen
			  • Stateful Inspection und Deep Packet Inspection
			  • Intrusion Detection/Prevention Systems (IDS/IPS)
			  • VPN-Zugänge mit starker Authentifizierung
			  • Netzwerkzugangskontrolle (NAC) zur Geräteprüfung vor Netzfreigabe
			• Organisatorische Massnahmen:
			  • Netzwerkzonenmodell dokumentieren
			  • Change-Management-Prozess für Firewall-Regeln
			  • Regelmässige Überprüfung der Segmentierungsstrategie
			  • Schulungen für Netzwerkadministratoren
			• Auf Auflistung von TOMs für Zero Trust / Minimal Trust-Ansatz wird hier verzichtet
					X

Schützen / Protect	Malwareschutz	Schutzobjekt (Arbeitsplatzgeräte, E-Mail, Internet, Server) muss mit geeigneten Massnahmen wirksam vor bösartiger Software (Malware) und Angriffen geschützt sein.	• Echtzeitschutz (Real-Time Protection), Endpoint Detection & Response (EDR oder XDR) zur Analyse und Isolation infizierter Systeme / Korrelation / autom. Reaktion • Permanente Überwachung von Dateien, Prozessen und Netzwerkverbindungen • Sofortige Reaktion auf verdächtige Aktivitäten / automatisierte Isolation • Verhaltensbasierte Erkennung (Behavioral Analysis) • Analyse von Prozessverhalten zur Erkennung unbekannter Malware (Zero-Day) • Sandboxing-Technologien zur sicheren Ausführung verdächtiger Dateien • Exploit- und Ransomware-Schutz • Schutz vor Speicher- und Skript-Exploits • Erkennung und Blockierung von Verschlüsselungsversuchen • Web- und E-Mail-Schutz		X

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
			• URL-Filterung, Phishing-Erkennung, Schutz vor Drive-by-Downloads, PROXY • Scannen von Anhängen und Links in E-Mails • Zentrale Verwaltung & Reporting • Integration in SIEM-Systeme (grössere Gemeinden)		
Schützen / Protect	Verschlüsselung und Löschung von Daten	Während ihrer Speicherung, Verarbeitung und Übertragung müssen Daten in Bezug auf ihre Vertraulichkeit und Integrität adäquat geschützt sein (z. B. mit Hilfe geeigneter kryptografischer Verfahren). Nicht mehr benötigte Daten müssen ihrem Schutzbedarf und regulatorischen Vorgaben entsprechend gelöscht werden.	• Verschlüsselung sensibler Daten auf Festplatten, Datenbanken und Backups (z. B. AES-256) • Zugriffsrechte nach dem Least-Privilege-Prinzip • Integritätsprüfungen (z. B. Hashes, Checksummen) • Sichere Schlüsselverwaltung (z. B. HSM, KMS) • Klassifizierung von Daten nach Schutzbedarf • Dokumentierte Richtlinien zur Datenhaltung • Regelmässige Überprüfung der Speicherorte und –sicherheit • Ende-zu-Ende-Verschlüsselung (z. B. TLS 1.3, HTTPS, VPN) • Authentifizierung und Integritätsprüfung (z. B. digitale Signaturen, HMAC) • Vermeidung unsicherer Protokolle (z. B. FTP, HTTP, Telnet) • Strategie für Post Quantum Cryptografie entwickeln • Sichere Datenlöschung bei Rückgabe Geräte / Festplatten		X
Schützen / Protect	Datensicherung	Alle für die wichtigen Geschäfts- und Produktionsprozesse relevanten Daten müssen regelmässig gesichert werden. Idealerweise ist dazu ein Backupkonzept umzusetzen, das eine Online/Offline-Datenhaltung in mehreren Generationen an mehreren Standorten vorsieht. Zudem müssen zu jedem Zeitpunkt (auch nach Komplettverlust / Verschlüsselung der produktiven Umgebung) die Daten möglichst zeitnah und vollständig wieder hergestellt werden können, und die	• Backup-Strategie & -Frequenz • Regelmässige Backups: z.B. täglich inkrementell, wöchentlich voll • Mindestens 3 Generationen aufbewahren (z. B. 7-14-30 Tage) • Schutz vor Ransomware & Manipulation • 3-2-1-Regel: 3 Kopien der Daten, 2 unterschiedliche Medien (z. B. NAS + Cloud), 1 Kopie offline oder unveränderbar (z. B. WORM, Air Gap) oder immutable Backups: Backups dürfen nach Erstellung nicht mehr verändert oder gelöscht werden oder air-Gapped oder Offline-Backups: Z. B. Festplatten / Tapes, die nur während des Backups verbunden sind • Zugriffsrechte strikt beschränken: Nur dedizierte Backup-Accounts mit minimalen Rechten • Backup-Software vom Produktivnetz trennen, mit separatem Zugang • Wiederherstellbarkeit sicherstellen • Regelmässige Restore-Tests: Mindestens vierteljährlich stichprobenartig prüfen • Dokumentation der Wiederherstellungsdauer und -qualität • Notfallwiederherstellungsplan (Disaster Recovery Plan):		X

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
		Datenwiederherstellung muss periodisch geübt werden.	• Klar definierte Abläufe, Verantwortlichkeiten und Kommunikationswege • Schnellwiederherstellung kritischer Systeme: • Z. B. durch Snapshots oder virtuelle Maschinen • Bei Cloud-Backup (optional, aber empfohlen) • Verschlüsselte Übertragung & Speicherung (z. B. AES-256, TLS) • Zugriffsschutz durch MFA & rollenbasierte Rechte • Georedundante Speicherung bei Cloud-Anbietern • Organisatorische Massnahmen • Backup-Richtlinie dokumentieren: • Was, wie oft, wohin, wie lange, wer ist verantwortlich • Schulung der IT-Verantwortlichen: Umgang mit Backup-Software, Restore-Prozesse, Ransomware-Erkennung • Monitoring & Alarmierung: Bei fehlgeschlagenen Backups oder ungewöhnlichem Verhalten		
Schützen / Protect	Entwicklung	Bei der Entwicklung von IT-Services muss die Cybersicherheit von Anfang an mitberücksichtigt werden. Einhalten von Richtlinien und Best Practices bei der Umsetzung (bzw. die Vermeidung von unsicheren Praktiken), kontinuierliche Sicherheitsprüfungen. In jedem Fall müssen Entwicklungs- und produktive Umgebungen getrennt werden.	• Erfüllung von "Best Practice" Herstellervorgaben, z.B. Zertifikatsinfrastruktur, Servereinstellungen, etc. • Erfüllung internationaler Vorgaben (z.B. CIS-Hardening) bei Windows, Linux, Webserver, Microsoft Office etc. • Secure Software (SSDLC Frameworks wie z.B OWASP SAMM, NIST SSDF oder Microsoft SDL) bei Lieferanten einfordern • zwingende Einhaltung und Testing von OWASP TOP 10 Prinzipien • Secret Management, keine Passwörter oder Zugänge auf Systemen oder im Code • Pentesting der Infrastruktur / Entwicklung		X
Schützen / Protect	Verfügbarkeit	Jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt muss im Hinblick auf seine Verfügbarkeit gesichert sein. Insbesondere müssen dazu genügend Rechen-, Speicher- und Übertragungskapazitäten vorhanden und wichtige Komponenten wann immer sinnvoll auch redundant sein.	• Ausreichende Ressourcen bereitstellen • Allenfalls redundante Hardware-Komponenten (z. B. Netzteile, Festplatten, Netzwerkkarten) und Cluster- oder Failover-Systeme für kritische Dienste oder Georedundante Systeme (z. B. in Cloud- oder Rechenzentrumsumgebungen) • RAID-Systeme für Speichersicherheit • Test der Failover-Funktionalität in regelmässigen Abständen • Für längerfristigen Totalausfall: Disaster Recovery Plan (DRP) und Notfallplan ("Papierprozesse") / Business Continuity Management (BCM), Notfallübungen • USV-Systeme (unterbrechungsfreie Stromversorgung) • Alerting bei Schwellenwertüberschreitungen • Log-Analyse zur Früherkennung von Ausfällen • 24/7-Bereitschaft oder Eskalationsplan		X

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
Entdecken / Detect	Aufzeichnung und Überwachung	Für jede Hard- und Softwarekomponente bzw. jedes aggregierte Informatikschutzobjekt müssen sicherheitsrelevante Aktivitäten, Vorfälle und Ereignisse aufgezeichnet und im Hinblick auf möglicherweise erfolgte Angriffe möglichst zeitnah und automatisiert ausgewertet werden.	• Logging-Richtlinie definieren (Was, wie lange, wo gespeichert) • Aktivierung von Logging auf allen relevanten Systemen und wegspeichern der Logs auf einen zentralen, gesicherten Speicher, sichere Aufbewahrung von Logs für forensische Analysen • Schutz der Logdaten vor Manipulation, Zugriffsrechte auf Logs beschränken • standardisierte Logformate (z. B. Syslog, JSON) nutzen • In grössere Gemeinden: Korrelation von Ereignissen zur Erkennung von Mustern und Angriffen nutzen, automatisierte Auswertung durch SIEM/SOC-Systeme • Regelbasiertes und verhaltensbasiertes Alerting		X
Entdecken / Detect	Meldestelle	Es muss klar sein, wie Aussenstehende Schwachstellen und sicherheitsrelevante Vorfälle melden können, wie auch von einem Vorfall betroffene Dienstleister. Zudem müssen interne Meldeabläufe klar sein.	• Prozess Meldung: Intern (sofort), falls Eskalation notwendig Support IT Dienstleister (sofort), Polizei (sofort), Bund https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/meldepflicht-info.html (innert 24h), Kanton security@ag.ch (sofort) • wenn externe Schwachstellen / Fehler sehen (z.B. security.txt hinterlegen) zwecks Kontaktaufnahme • wenn Dienstleister betroffen: Vertraglich sicherstellen, dass sich DL sehr zeitnah meldet (Datenschutzverletzung, Informationssicherheitsrisiken?)		X
Reagieren / Respond	Eingrenzung	Im Falle eines Sicherheitsvorfalls müssen Massnahmen zur schnellen Eindämmung und koordinierten Wiederherstellung greifen, um Auswirkungen auf Geschäftsprozesse so gering wie möglich zu halten	• Automatisierte und manuelle, schnelle Reaktion IT-Dienstleister zwecks schneller Eingrenzung des Schadensausmass • Segmentierung, damit Schaden sich nicht ausbreitet • Schäden minimieren • Kontrollierte Isolation (nicht herunterfahren zwecks Forensik) • Eskalationspfade sind definiert		X

Bereich	Thema	Anforderung	mögl. Massnahmen und TOMs	GL	IT
Reagieren / Respond	Untersuchung	Für zu erstellenden Notfallpläne müssen die Verantwortlichkeiten und Zielsetzungen der Kommunikation bekannt sein.	• Wie kam es dazu • Lesson learned • Reporting Vorfall und Massnahmen definieren	X	X
Wiederherstellen / Recover	Notfallplanung	Die Wiederherstellung der Betriebsfähigkeit muss sichergestellt sein. Mit oder ohne IT. Dazu müssen Notfallpläne und entsprechende Prozesse definiert, priorisiert, regelmässig geübt und gegebenenfalls auch verbessert werden.	• Business Impact Analyse (BIA) erstellen: Identifikation kritischer Geschäftsprozesse • Notfallplan: wie weiter ohne IT (2-3 Tage, 2-3 Wochen?) • Wiederanlaufplanung • Notfallarbeitsplätze (z. B. Homeoffice, Ausweichstandorte) • USV & Notstromversorgung für kritische Infrastruktur • Kontaktlisten & Eskalationswege (intern & extern) • Vertragliche Regelungen mit Dienstleistern (z. B. SLAs, Notfallzugänge, Notfallpasswörter) • Zentrale Ablage aller Notfalldokumente (digital & physisch) • Regelmässige Aktualisierung (mind. jährlich oder bei Änderungen) • Zugriffskontrolle & Schutz der Notfalldokumentation	X	
Wiederherstellen / Recover	Kommunikation	Für zu erstellenden Notfallpläne müssen die Verantwortlichkeiten und Zielsetzungen der Kommunikation bekannt sein.	• Sicherstellen, dass alle Mitarbeitenden wissen, wie sie im Notfall informiert werden • Intern: Geschäftsleitung, IT, Mitarbeitende • Extern: Kunden (Einwohnende), Partner / Behörden (Kanton, KAPO, Bund, EW, GAS, Wasser), Lieferanten, Medien • Kommunikationskanäle bestimmen • Kommunikationsplan im Notfallhandbuch verankern, Vorlagen vorbereiten • Verantwortlichkeiten klar zuweisen: Wer informiert wen, wann und wie? • Wer spricht mit der Presse oder Behörden? • Notfallkontaktliste pflegen (inkl. Mobilnummern, Privatnummern) • Offline-Kopie der Kontaktliste (z. B. ausgedruckt oder auf USB-Stick) • Alternative Kommunikationsmittel • Kommunikationsübungen im Rahmen von Notfalltests	X	

3.2 Technische Vorgaben Authentifizierung

Als Vorschlag für elektronische Zugänge kann folgende Tabelle ihrem IT-Dienstleister zur Verfügung gestellt werden:

Sicherheitsstufe	**Authentifizierungsvorgaben**
tief	Benutzername und Passwort (wenn extern erreichbar, mit MFA absichern) 12 -14 Zeichen komplex (allenfalls "Passwordless oder Passphrase" einführen)
mittel	• Benutzername und Passwort mit SMS-Verifikationscode • 16 Zeichen random • Benutzername und Passwort mit Gerätebindung* • OTP-Softwarelösung (z. B. Google oder Microsoft Authenticator) • Software-Zertifikats-basierte Authentifikation im Rahmen von TLS* • FIDO2-Implementierungen mit Synchronisations- und Schlüsselexportiermöglichkeiten (z. B. Passkeys*) • Kerberos-Tickets • SAML- und OIDC-Token
hoch	• 24+ Zeichen random • OTP-Token (z.B. RSA, Vasco, …) • OTP-Lösung auf der Basis eines TPM* • Hardware-Zertifikats-basierte Authentifikation im Rahmen von • TLS* • FIDO2-Implementierungen ohne Synchronisations- und Schlüsselexportiermöglichkeiten* • Swisscom Mobile ID • Kerberos-Tickets und andere Tokens, die auf der Basis einer Authentifikation der Stufe hoch ausgestellt worden sind

3.3 Minimal-Checkliste zur Cyberresilienz für kleinere Gemeinden

Nr.	Thema	Ziel / Beschreibung	Erledigt (X)
1	Sicherheitsverantwortung klären	Gibt es eine Ansprechperson für Informationssicherheit (intern und/oder bei einem Dienstleister)?	
2	Schulung aller Mitarbeitenden	Haben Mitarbeitende Schulungen zu Phishing, Passwörtern, Datenumgang erhalten? (z. B. elearningcyber.ch)	
3	Multi-Faktor-Authentifizierung (MFA)	Sind externe Zugänge (z. B. Mailsystem, Remote-Zugriff) mit MFA abgesichert?	
4	Sicheres und getestetes Backup	Gibt es regelmässige Backups, die offline/unveränderbar sind und wurde die Wiederherstellung getestet?	
5	Virenschutz & automatische Updates	Ist ein aktueller Virenschutz vorhanden und werden Schwachstellen (Patches) regelmässig behoben?	
6	Externe Dienstleister vertraglich verpflichtet	Sind Sicherheitsanforderungen und Meldepflichten bei IT-Dienstleistern vertraglich geregelt?	
7	Notfallplan vorhanden	Gibt es ein Notfallkonzept (z. B. für Systemausfall, Verschlüsselung, Cyberangriff)?	
8	Schutzbedarf der Daten analysiert	Wurden zentrale Systeme/Daten klassifiziert (z. B. vertraulich, sensibel, öffentlich)?	
9	Netzwerkzugänge kontrolliert	Ist der Zugang zum Netzwerk (intern & extern) kontrolliert (z. B. Gäste, Externe, WLAN)?	
10	GAP-Analyse durchgeführt	Wurde der aktuelle Stand zur Informationssicherheit überprüft (z. B. mit IKT-Minimalstandard)?	