GEMEINDE
WEISSLINGEN

Referenz-Nr. WISLIG-2021-0359

Mehrjahresplanung Audits Datenschutz

der Gemeinde Weisslingen

Datum	29. Januar 2026
Ordnungsnummer	301.113

SILVANO BENVENUTO CASTIONI

Digital signiert von: SILVANO BENVENUTO CASTIONI
Name: CN = SILVANO BENVENUTO CASTIONI C = CH
Datum: 2026.02.10 08:56:32 + 01'00'

Gemeindeverwaltung Weisslingen
Dorfstrasse 40 · Postfach 218 · 8484 Weisslingen · Telefon 052 397 31 00 · www.weisslingen.ch

Inhaltsverzeichnis

1. Zweck der Mehrjahresplanung

Diese Mehrjahresplanung legt die **systematische, risikobasierte und gesetzeskonforme Durchführung von IT-Sicherheits- und Datenschutzüberprüfungen** der Gemeinde Weisslingen fest. Sie stellt sicher, dass die Vorgaben aus:

- den Richtlinien für Informationssicherheit und Datenschutz (Ordnungsnummer 301.11),
- dem Informationssicherheitskonzept,
- dem Gesetz über die Information und den Datenschutz (IDG),
- sowie der Leitlinie Informationssicherheit des Kantons Zürich

kontinuierlich überprüft und weiterentwickelt werden.

Die Planung dient als Steuerungsinstrument für Gemeinderat, Geschäftsleitung und Informationssicherheitsverantwortliche bzw. -verantwortlicher (ISV).

2. Audit-Grundsätze

Die Audits erfolgen nach folgenden Grundsätzen:

- **Mehrjähriger Audit-Zyklus (4 Jahre)** gemäss Richtlinien
- **Risikobasierter Ansatz** (kritische Systeme häufiger)
- Kombination aus:
  - organisatorischen Audits,
  - technischen Audits,
  - Datenschutz- und Compliance-Prüfungen
- Einsatz **unabhängiger interner oder externer Stellen**
- Nachvollziehbare Dokumentation und Massnahmenverfolgung

3. Audit-Typen

Nachfolgende Audit-Typen solle zur Anwendung kommen:

Audit-Typ	Inhalt	Durchführung
Organisations- und Governance-Audit	Rollen, Prozesse, Richtlinien, Schulungen	extern / intern unabhängig
Technisches IT-Sicherheitsaudit	Infrastruktur, Netzwerke, Systeme	extern
Datenschutz-Audit	IDG-Konformität, Betroffenenrechte, DSFA	extern / kantonal
Applikationsspezifisches Audit	Fachanwendungen mit Personendaten	risikobasiert
Notfall- und Resilienztest	Backup, Wiederherstellung, Notfallorganisation	intern und extern

4. Mehrjahresplanung (4-Jahres-Zyklus)

Die Mehrjahresplanung wird mit der Legislatur synchronisiert. Das heisst, dass der Zyklus jeweils am 1. Juli beginnt, erstmalig am 1. Juli 2026.

Jahr 1 – Basis- und Governance-Audit

Ziel: Gesamtüberblick, Reifegradbestimmung

Prüfungsinhalte:

- Informationssicherheitskonzept und Richtlinien
- Rollen (ISV, DSBr, ADV) und Organisation
- Schulungs- und Sensibilisierungsmassnahmen
- Ausnahme- und Incident-Management
- Dokumentation und Inventare

Auditform:
— Externes Organisations- und Governance-Audit

Ergebnis:
— Reifegradbericht
— Massnahmenplan mit Priorisierung

Jahr 2 – Technisches IT-Sicherheitsaudit

Ziel: Überprüfung der technischen Schutzmassnahmen

Prüfungsinhalte:
— Netzwerksicherheit (Firewall, VPN, Segmentierung)
— Server-, Client- und Cloud-Umgebungen
— Patch- und Vulnerability-Management
— Authentifizierung (inkl. MFA)
— Logging und Monitoring

Auditform:
— Externes technisches Audit / Schwachstellenanalyse

Ergebnis:
— Technischer Auditbericht
— Konkrete Härtungs- und Umsetzungsmaßnahmen

Jahr 3 – Datenschutz- und Applikationsaudit

Ziel: Sicherstellung der IDG- und Datenschutzkonformität

Prüfungsinhalte:
— Bearbeitung von Personendaten
— Datenschutz-Folgenabschätzungen
— Auskunfts-, Lösch- und Sperrprozesse
— Kritische Fachapplikationen (z. B. FIS/Abacus, Tutoris, Spidersoft, GemDat)
— Outsourcing- und Cloud-Verträge

Auditform:
— Externes Datenschutz- und Applikationsaudit

Ergebnis:
— Datenschutzbericht
— Empfehlungen zur Optimierung von Prozessen und Verträgen

Jahr 4 – Notfall-, Wiederherstellungs- und Wirksamkeitsprüfung

Ziel: Überprüfung der Resilienz und Wirksamkeit

Prüfungsinhalte:
— Notfallkonzept und Eskalationsprozesse
— Backup- und Restore-Tests (RTO/RPO)
— Incident-Response-Übungen
— Überprüfung der Umsetzung früherer Massnahmen

Auditform:
— Kombiniertes intern/extern begleitetes Audit

Ergebnis:
— Wirksamkeitsnachweis
— Entscheidungsgrundlage für nächsten Audit-Zyklus

5. Laufende jährliche Aktivitäten (zusätzlich)

Unabhängig vom Zyklus werden jährlich durchgeführt:

- Review der Zugriffsrechte (mind. jährlich)
- Überprüfung administrativer Berechtigungen (halbjährlich)
- Schulungsnachweis und Sensibilisierung
- Überprüfung der Ausnahmebewilligungen
- Aktualisierung Risikoanalyse

6. Rollen und Verantwortlichkeiten

Rolle	Verantwortung
Gemeinderat	Kenntnisnahme der Ergebnisse
Geschäftsleitung	Steuerung und Priorisierung
ISV	Koordination, Massnahmenverfolgung
DSBr	Datenschutz-Compliance
Externe Prüfstelle	Unabhängige Auditdurchführung

7. Berichterstattung und Nachverfolgung

- Jeder Audit schliesst mit einem schriftlichen Bericht
- Massnahmen werden:
- priorisiert,
- terminiert,
- verantwortlichen Rollen zugewiesen
- Umsetzung wird durch den ISV überwacht
- Statusbericht mindestens jährlich an die Geschäftsleitung

8. Genehmigung

Diese Mehrjahresplanung wird durch die Geschäftsleitung genehmigt und dem Gemeinderat zur Kenntnis gebracht.

Gemeinde Weisslingen

Silvano Castioni
Gemeindeschreiber