

Informationssicherheitskonzept

der Gemeinde Weisslingen

Datum 29. Januar 2026

Ordnungsnummer 301.112

Inhaltsverzeichnis

1.	Zweck und Einordnung	3
2.	Grundlagen und Referenzdokumente	3
3.	Geltungsbereich	3
4.	Informationssicherheitsniveau	3
5.	Informationssicherheitsziele	3
6.	Informationssicherheitsorganisation	4
6.1	Grundsatz	4
6.2	Rollen und Verantwortlichkeiten	4
7.	Steuerung und Governance	4
7.1	Ausnahmenmanagement	4
7.2	Kontinuierliche Verbesserung	4
8.	Umsetzung der Informationssicherheitsmassnahmen	5
9.	Risikoanalyse und Notfallmanagement	5
10.	10. Inkraftsetzung	5

1. Zweck und Einordnung

1. Dieses Informationssicherheitskonzept beschreibt die konkrete Umsetzung, Steuerung und Weiterentwicklung der Informationssicherheit in der Gemeinde Weisslingen. Es basiert verbindlich auf den Richtlinien für Informationssicherheit und Datenschutz der Gemeinde Weisslingen¹ und operationalisiert diese.
2. Das Konzept dient insbesondere:
 - als Führungs- und Steuerungsinstrument für Gemeinderat und Geschäftsleitung,
 - als Umsetzungsrahmen für organisatorische und technische Massnahmen,
 - als Nachweis gegenüber Aufsichts- und Prüfstellen.
3. Das Konzept ergänzt die Richtlinien, ersetzt diese jedoch nicht.

2. Grundlagen und Referenzdokumente

4. Dieses Informationssicherheitskonzept stützt sich auf:
 - Richtlinien für Informationssicherheit und Datenschutz der Gemeinde Weisslingen und die darin aufgeführten weiteren Grundlagen
 - Leitlinie zur Informationssicherheit der Gemeinde Weisslingen
 - IT-Strategie der Gemeinde Weisslingen

3. Geltungsbereich

5. Das Informationssicherheitskonzept gilt für:
 - alle Organisationseinheiten der Gemeindeverwaltung Weisslingen,
 - alle Mitarbeitenden, Behörden- und Kommissionsmitglieder,
 - externe Dienstleister und Vertragspartner mit Zugriff auf Informationen der Gemeinde.
6. Es umfasst alle Informationen unabhängig von Form und Trägermedium (elektronisch, physisch, mündlich).

4. Informationssicherheitsniveau

7. Die Gemeinde Weisslingen verfolgt ein **normales Informationssicherheitsniveau**. Diese Einstufung basiert auf:
 - der Bearbeitung von Personendaten und besonderen Personendaten,
 - der vollständigen Abhängigkeit zentraler Verwaltungsprozesse von IT-Systemen,
 - der Notwendigkeit einer hohen Verfügbarkeit bei vertretbaren Restrisiken.
8. Schutzmassnahmen werden risikobasiert, verhältnismässig und nach dem Stand der Technik umgesetzt.

5. Informationssicherheitsziele

9. Die Gemeinde Weisslingen verfolgt folgende übergeordnete Ziele:
 - **Vertraulichkeit:** Schutz vor unbefugtem Zugriff und Kenntnisnahme
 - **Integrität:** Schutz vor unbefugter oder unbeabsichtigter Veränderung
 - **Verfügbarkeit:** Sicherstellung der Nutzbarkeit bei Bedarf
 - **Nachvollziehbarkeit:** Lückenlose Protokollierung sicherheitsrelevanter Vorgänge
 - **Zurechenbarkeit:** Eindeutige Zuordnung von Bearbeitungshandlungen
 - **Rechtskonformität:** Einhaltung aller gesetzlichen Vorgaben

¹ WSR 301.11

6. Informationssicherheitsorganisation

6.1 Grundsatz

10. Die Informationssicherheitsorganisation ist verbindlich in den Richtlinien definiert und im Anhang dokumentiert. Zuständigkeiten, Stellvertretungen und Anwendungen sind eindeutig zugeordnet.

6.2 Rollen und Verantwortlichkeiten

11. Gemeinderat Weisslingen

- Oberste Verantwortung für Informationssicherheit
- Kenntnisnahme der Richtlinien und Konzepte

12. Geschäftsleitung / Gemeindeschreiberin bzw. Gemeindeschreiber

- Operative Gesamtverantwortung
- Durchsetzung und Kontrolle der Vorgaben

13. Informationssicherheitsverantwortliche bzw. Informationsverantwortlicher (ISV)

- Zentrale Koordinations- und Kontrollfunktion
- Umsetzung, Überwachung und Weiterentwicklung der Informationssicherheit
- Behandlung von Ausnahmen und Sicherheitsvorfällen

14. Datenschutzberaterin bzw. Datenschutzberater (DSBr)

- Fachliche Verantwortung für Datenschutz
- Kontaktstelle zur kantonalen Datenschutzbeauftragten

15. Anwendungs- und Datenverantwortliche bzw. -verantwortlicher (ADV)

- Verantwortung für Anwendungen, Datenklassifikation, Zugriffe und Betrieb

16. Mitarbeitende

- Einhaltung aller Vorgaben
- Meldung von Sicherheits- und Datenschutzvorfällen

7. Steuerung und Governance

7.1 Ausnahmenmanagement

17. Abweichungen von Richtlinien und Weisungen:
- bedürfen der Genehmigung durch den ISV,
 - sind schriftlich zu begründen,
 - zeitlich zu befristen und zu dokumentieren,
 - periodisch zu überprüfen.

7.2 Kontinuierliche Verbesserung

18. Die kontinuierliche Verbesserung beinhaltet:
- Überprüfung der Richtlinien und dieses Konzepts mindestens alle **vier Jahre**
 - zusätzliche Überprüfungen bei wesentlichen organisatorischen oder technischen Änderungen
 - regelmässige unabhängige Prüfungen

8. Umsetzung der Informationssicherheitsmassnahmen

19. Die operativen Massnahmen ergeben sich direkt aus den Richtlinien und werden insbesondere durch folgende Instrumente umgesetzt:
- Rollen- und Berechtigungskonzept (IT-Betreiber und Gemeinde)
 - Schulungs- und Sensibilisierungsprogramm (Gemeinde)
 - Mobile- und Homeoffice-Regelungen (Gemeinde)
 - Passwort- und Authentifizierungsvorgaben (IT-Betreiber)
 - Datensicherungs- und Wiederherstellungsstrategie (IT-Betreiber)
 - Physische Sicherheitsmassnahmen (IT-Betreiber und Gemeinde)
 - Incident- und Notfallmanagement (IT-Betreiber)
20. Die detaillierte Umsetzung erfolgt in Weisungen, technischen Richtlinien und Prozessbeschreibungen.

9. Risikoanalyse und Notfallmanagement

21. Schwerpunkte sind:
- Durchführung und Pflege einer Auswirkungs- und Bedrohungsanalyse
 - Ableitung angemessener Schutz- und Notfallmassnahmen
 - Definition von Recovery Time Objective, (RTO)- und Recovery Point Objectiv (RPO)-Werten für kritische Systeme
 - regelmässige Tests der Notfallorganisation

10. Inkraftsetzung

22. Dieses Informationssicherheitskonzept tritt mit Genehmigung durch die Geschäftsleitung in Kraft und wird dem Gemeinderat zur Kenntnis gebracht.

Gemeinde Weisslingen

Silvano Castioni
Gemeindeschreiber