GEMEINDE
WEISSLINGEN

Referenz-Nr. WISLIG-2021-0359

Leitlinie zur Informationssicherheit

der Gemeinde Weisslingen

Datum	21. Oktober 2025
Ordnungsnummer	301.10

SILVANO
BENVENUTO
CASTIONI

Digital signiert von: SILVANO BENVENUTO CASTIONI
Name: CN = SILVANO BENVENUTO CASTIONI C = CH
Datum: 2025.10.24 11:27:54 + 02'00'

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

Inhaltsverzeichnis

1. Einleitung und allgemeine Bestimmungen

Art. 1 Rechtsetzung

Die Gemeinde Weisslingen ist zur Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie abhängig. Zur Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit, Nachvollziehbarkeit und Authentizität der Informationen und deren Verarbeitungssysteme nach § 7 Gesetz über die Information und den Datenschutz (IDG[1]) verabschiedet der Gemeinderat diese Leitlinie zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Gemeinde Weisslingen angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Leitlinie eine Beschreibung der Informationssicherheitsorganisation.

Art. 2 Geltungsbereich

Die Leitlinie zur Informationssicherheit und die damit zusammenhängenden Dokumente gelten für alle Mitarbeitenden der Gemeinde sowie für Behörden- und Kommissionsmitglieder. Vertragspartner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

2. Informationssicherheit

Art. 3 Informationssicherheitsniveau

1 Der Gemeinderat legt das Informationssicherheitsniveau so fest, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung ist eine Gefährdungsabschätzung über die Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit.

2 Für Datensammlungen mit einem höheren Schutzbedarf werden zusätzliche Sicherheitsmassnahmen getroffen.

Art. 4 Informationssicherheitsziele

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele (§ 7 IDG):

Integrität	Informationen müssen richtig und vollständig sein.
Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.
Verfügbarkeit	Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Verwaltungsbetrieb haben.
Vertraulichkeit	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
Zurechenbarkeit	Informationsbearbeitungen müssen einer Person zugerechnet werden können.
Verantwortung	Die politischen Behörden und die Mitarbeitenden der Gemeinde sind sich ihrer Verantwortung beim Umgang mit Informationen, IKT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.

Art. 5 Informationssicherheitsmassnahmen

Die Auswahl der technischen und organisatorischen Massnahmen erfolgt anhand der Anforderungen der ISO/IEC 27001 und den Standards des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI):

[1] LS 170.4

Aktualisierungen (Updates)	Alle IKT-Systeme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellsten Sicherheitsupdates versorgt.
Archivierung / Löschung	Alle Daten werden gemäss den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht.
Berechtigungskonzept	Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen der Behördenmitglieder, der Mitarbeitenden sowie der Lernenden auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben erforderlich und geeignet.
Datenschutz	Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen.
Datensicherung (Backup)	Die Datensicherung wird regelmässig durchgeführt. Die Sicherungsmedien werden an getrennten Orten aufbewahrt und sind physisch geschützt. Es wird gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.
IKT-Systeme	Die IKT-Systeme werden nach der Beschaffung sicher installiert (gemäss anerkannten Sicherheitsstandards) und betrieben, mittels eines Änderungsmanagements verwaltet und in einem geregelten Prozess ausser Betrieb genommen.
Mobile Geräte / Software	Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten (Bring Your Own Device) sowie der Installation von Software auf Arbeitsplatzrechnern und Servern sind im Detail geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.
Überwachung (Monitoring)	Die Verfügbarkeit und Qualität der Anwendungsdienste werden laufend überprüft.
Netzwerk / Firewall	Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern. Die vom Kanton vorgegebene Network Security Policy der übergeordneten Netzwerke (Leunet) wird eingehalten.
Organisation	Die relevanten Funktionen der Organisation sind festgelegt und in einem Organigramm dokumentiert. Für alle Funktionen ist die Stellvertretung geregelt. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe erfüllen können.
Outsourcing	Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart werden.
Passwörter	Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt.
Sensibilisierung / Schulung	Die Mitarbeiterinnen und Mitarbeiter nehmen jährlich an einer internen Sicherheitsschulung der für die Informationssicherheit verantwortlichen Person teil. Sie werden regelmässig über aktuelle Gefahren und zu treffende Massnahmen informiert.

Verschlüsselung	Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt verschlüsselt über öffentliche Netze.
Virenschutz / Internet	Virenschutzprogramme werden auf allen IKT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.
Weisungen	Die Mitarbeiterinnen und Mitarbeiter werden angewiesen, die Gesetze sowie die vertraglichen Regelungen und internen Richtlinien einzuhalten. Sie unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmassnahmen. Informationssicherheitsfragen und Hinweise auf Schwachstellen werden an die für die Informationssicherheit verantwortliche Person gerichtet.
Zutritt	Gebäude und Räume sowie IKT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.
Physische Sicherheit	Brandschutzmassnahmen, Zutrittskontrolle usw.

3. Informationssicherheitsorganisation

Art. 6 Gemeinderat

Der Gemeinderat trägt die Gesamtverantwortung für die Informationssicherheit der Gemeinde Weisslingen. Er legt die Leitlinie zur Informationssicherheit fest und genehmigt die für die Informationssicherheit erforderlichen Massnahmen und Mittel.

Art. 7 Gemeindeschreiberin bzw. Gemeindeschreiber

1 Die Gemeindeschreiberin bzw. der Gemeindeschreiber trägt die operative Verantwortung für die Informationssicherheit der Gemeinde.

2 Sie bzw. er bestimmt eine für Informationssicherheit und eine für Datenschutz verantwortliche Person oder übt diese Funktion(en) selbst aus.

3 Sie bzw. er stellt sicher, dass die Beschlüsse des Gemeinderats zur Informationssicherheit umgesetzt werden.

Art. 8 Informationssicherheitsverantwortliche bzw. Informationssicherheitsverantwortlicher (ISV)

1 Zur Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus wird eine Person bestimmt, die für die Informationssicherheit verantwortlich ist. Sie ist für die Ausarbeitung und Nachführung eines Sicherheitskonzepts verantwortlich und berichtet in dieser Funktion direkt der ihr oder ihm vorgesetzten Stelle.

2 Der oder dem ISV werden ausreichende finanzielle und zeitliche Ressourcen für die Ausübung der Tätigkeit zur Verfügung gestellt. Die IKT- und Anwendungsverantwortlichen sowie die IKT-Benutzerinnen und -Benutzer unterstützen sie bzw. ihn in ihrer bzw. seiner Tätigkeit. Sie bzw. er wird in alle Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

3 Für sicherheitsrelevante Fragen ist die bzw. der ISV weisungsberechtigt. Sie bzw. er ist die Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Art. 9 Anwendungs- und Datenverantwortliche bzw. -verantwortlicher (ADV)

Für alle Prozesse, Daten, Anwendungen, IKT- und Netzwerksysteme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf (Klassifizierung) bestimmt und die Zugriffsberechtigungen vergibt.

Art. 10 Datenschutzberaterin bzw. Datenschutzberater (DSBr)
Der Datenschutz und die Informationssicherheit sind für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, von grundlegender Bedeutung. Zur Umsetzung des Datenschutzes wird eine Person bestimmt, die für den Datenschutz verantwortlich ist. Die bzw. der DSBr arbeitet in dieser Rolle eng mit der bzw. den ISV zusammen und ist interne Ansprechperson bei Datenschutzfragen.

4. Kontinuierliche Verbesserung der Informationssicherheit

Art. 11 Überprüfung der Richtlinien
Der Gemeinderat unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Er gibt mit der periodischen Überarbeitung dieser Leitlinie zur Informationssicherheit die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung. Die Leitlinie ist alle vier Jahre zu überprüft.

Art. 12 Überprüfung des Informationssicherheitskonzepts

1 Das Informationssicherheitskonzept und deren Umsetzung wird regelmässig alle vier Jahre sowie zusätzlich bei Projekten mit grossen Auswirkungen auf den Datenschutz und Informationssicherheit auf die Aktualität und die Wirksamkeit geprüft. Festgestellte Abweichungen werden innert nützlicher Frist behoben.

2 Die zu ergreifenden Massnahmen orientieren sich am Stand der Technik sowie an nationalen und internationalen Standards.

5. Schlussbestimmungen

Art. 13 Inkraftsetzung
Die Leitlinie zur Informationssicherheit tritt per 1. Januar 2026 in Kraft.

Gemeinderat Weisslingen

Pascal Martin
Gemeindepräsident

Silvano Castioni
Gemeindeschreiber