Vorlage

Leitlinie zur Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000

Erläuterung zur Vorlage

Die vorliegende Vorlage Leitlinie zur Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000 ist Teil einer Vorlagenreihe, die sämtliche relevanten Informationssicherheitsdokumente umfasst. Die empfohlene Vorgehensweise, die Hilfestellungen und die Erläuterungen zu den Vorlagen sind dem [Leitfaden Informati­onssicherheit in Gemeinden – Bevölkerungszahl > 6000](https://docs.datenschutz.ch/u/d/informationssicherheit/gemeinden/leitfaden_informationssicherheit_gemeinden_groesser_6000.pdf) zu entnehmen.

Die Vorlage ist den jeweiligen Gegebenheiten anzupassen. Die anzupassenden Punkte befinden sich in ecki­gen Klammern [ ].

Der Leitfaden Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000, die Vorlagen und weitere Dokumente sind auf [www.datenschutz.ch](https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/informationssicherheit) publiziert.

Änderungskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung, Bemerkung | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Leitlinie zur Informationssicherheit [Gemeinde/Stadt]

# Einleitung

Die [Gemeinde/Stadt] 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, [LS 170.4](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4)) verabschiedet der [Gemeinderat/Stadtrat] diese Leitlinie zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der [Gemeinde/Stadt] angestrebte Informationssicher­heitsniveau, die Informationssicherheitsziele sowie die geeigne­ten Massnahmen definiert. Weiter beinhaltet die Leitlinie eine Beschreibung der Informationssicherheitsor­ganisation.

# Geltungsbereich

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

# Informationssicherheitsniveau

Der [Gemeinderat/Stadtrat] der [Gemeinde/Stadt] hat entschieden, dass ein angemessenes Sicherheitsniveau für einen normalen Schutzbedarf angestrebt werden soll. Grundlage für diese Entscheidung war eine Gefährdungsabschätzung über die Werte der Schutzobjekte sowie des vertretbaren Aufwands an Personal und Finanzmitteln für Informationssicherheit. Für Datensammlungen mit einem höheren Schutzbedarf werden zusätzliche Sicherheitsmassnahmen getroffen.

# 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. |
| **Verantwortung** | Die politischen Behörden und die Mitarbeitenden der [Gemeinde/Stadt] sind sich ihrer Verantwortung beim Umgang mit Informationen, IKT-Syste­men und Anwendungen bewusst. Sie unterstützen die Informa­tions­si­cherheitsziele. |
| **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. |

# Informationssicherheitsmassnahmen

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

| 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 mindestens 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. |

# Informationssicherheitsorganisation

Die Gemeindeschreiberin/der Gemeindeschreiber beziehungsweise die Stadtschreiberin/der Stadtschreiber, die Informationssicherheitsverantwortliche oder der In­formationssicherheitsverantwortliche und die für die einzelnen Bereiche zuständigen Daten- und Anwen­dungsverantwortlichen haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

Die Informationssicherheitsorganisation ermöglicht es der [Gemeinde/Stadt], das angestrebte Informations­sicher­heitsniveau zu erreichen und dieses aufrechtzuerhalten. Informierte und geschulte Mitarbeitende sind die Voraussetzung dafür, dass die [Gemeinde/Stadt] die gesteckten Informationssicherheitsziele erreichen können. Auf ihre Sensibilisierung und Weiterbildung ist besonderes Gewicht zu legen.

## Gemeinderat/Stadtrat

Der Gemeinderat/der Stadtrat trägt die Gesamtverantwortung für die Informationssicherheit der [Gemeinde/Stadt]. Er legt die Leitlinie zur Informationssicherheit fest und genehmigt die für die Informa­tions­sicherheit erforderlichen Massnahmen und Mittel.

Gemeindeschreiberin/Gemeindeschreiber / Stadtschreiberin/Stadtschreiber

Die Gemeindeschreiberin/der Gemeindeschreiber beziehungsweise die Stadtschreiberin/der Stadtschreiber trägt die operative Verantwortung für die Informationssi­cherheit der [Gemeinde/Stadt]. Sie/er bestimmt eine für Informationssicherheit und eine für Datenschutz verant­wortliche Person oder übt diese Funktion(en) selbst aus und stellt sicher, dass die Beschlüsse des Gemeinde­rats/Stadtrats zur Informationssicherheit umgesetzt werden.

Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher (ISV)

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.

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/ihn in ihrer/seiner Tätigkeit. Sie/er wird in alle Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

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

Anwendungs- und Datenverantwortliche

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

Datenschutzberaterin/Datenschutzberater

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 Datenschutzberaterin/der Datenschutzberater ar­beitet in dieser Rolle eng mit den Informationssicherheitsverantwortlichen zusammen und ist interne An­sprechperson bei Datenschutzfragen.

# Kontinuierliche Verbesserung der Informationssicherheit

Der [Gemeinderat/der Stadtrat] 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 wird alle [FRIST VON 1–3 WÄHLEN] Jahre überprüft.

Das Informationssicherheitskonzept und deren Umsetzung wird regelmässig alle [FRIST VON 1–2 WÄHLEN] 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.

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

Beschlossen vom [Gemeinderat/Stadtrat] mit Beschluss [NR.] am [DATUM]

[ORT UND DATUM] [NAME]

[Gemeinde/Stadt] Gemeindeschreiberin/Gemeindeschreiber / Stadtschreiberin/Stadtschreiber

V 4.4 / Oktober 2024