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 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://www.datenschutz.ch/) publiziert.

Leitlinie zur Informationssicherheit [GEMEINDE]

# Einleitung

Die [GEMEINDE] 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=170.4,12.02.2007,01.10.2008,109)) verabschiedet der Gemeinderat diese Leitlinie zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der [GEMEINDE] 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 (insbesondere das Rollen- und Berechtigungskonzept, das Sicherheitskonzept, die Informationssicherheitsorganisation und die Anleitung Sensibilisierung der Mitarbeitenden) gelten für alle Mitarbeitenden der [GEMEINDE]. Vertrags­partner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen ver­pflichtet.

# Informationssicherheitsniveau

Das Informationssicherheitsniveau der [GEMEINDE] entspricht der «Schutzstufe 1 – Grundschutz» gemäss Allgemeiner Informationssicherheitsrichtlinie AISR der kantonalen Verwaltung. Diese Einstufung erfolgt auf­grund der Tatsache, dass die Anzahl der betroffenen Personen mittel ist, alle wesentlichen Funktionen und Aufgaben durch IT- und Netzwerksysteme unterstützt werden und ein Ausfall von IT- und Netzwerksystemen die Aufgabenerfüllung nicht beeinträchtigen darf. Die [GEMEINDE] bearbeitet auch Daten, die einen erhöh­ten Schutz vor unberechtigten Zugriffen und von unerlaubten Änderungen benötigen.

# 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 sind sich ihrer Verantwortung beim Umgang mit Informationen, IT-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

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Massnahmen:

|  |  |
| --- | --- |
| Aktualisierungen / Updates | Alle IT-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 Behördenmitglieder, für Mitar­beitende sowie für Lernende auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben geeignet und erforderlich. |
| **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 (Back-up)** | 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. |
| **IT-Systeme** | Die IT-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. |
| **Monitoring / Überwachung** | 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 Datensicherheit 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** | 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 IT-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 IT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt. |
| **Physische Sicherheit** | Brandschutzmassnahmen usw. |

# Informationssicherheitsorganisation

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

Die Informationssicherheitsorganisation der [GEMEINDE] ist im Anhang A – Organigramm [GEMEINDE] definiert.

## Informationssicherheitsverantwortung

Gemeinderat

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

Gemeindeschreiberin / Gemeindeschreiber

Die Gemeindeschreiberin / der Gemeindeschreiber trägt die operative Verantwortung für die Informationssi­cherheit der [GEMEINDE]. 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 zur Informationssicherheit umgesetzt werden.

Informationssicherheitsverantwortliche / Informationssicherheitsverantwortlicher

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 Informationssicherheitsverantwortlichen werden ausreichende finanzielle und zeitliche Res­sourcen für die Ausübung ihrer Tätigkeit zur Verfügung gestellt. Die IT- und Anwendungsverantwortlichen sowie die IT-Benutzerinnen und IT-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 Informationssicherheitsverantwortliche weisungsberechtigt. Sie ist die Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen und verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten.

Aufgaben der / des Informationssicherheitsverantwortlichen:

* Initialisieren, überwachen und kontrollieren der Leitlinie zur Informationssicherheit
* Führen des Inventars über die Schutzobjekte
* Erstellen, überarbeiten und überprüfen der Sicherheitsvorgaben (Leitlinie zur Informationssicherheit, Informationssicherheitskonzept, Weisungen, Merkblätter usw.)
* Kontrollieren des Fortschritts der Umsetzung von Informationssicherheitsmassnahmen
* Berichten an die Gemeindeschreiberin / den Gemeindeschreiber über den Stand der Informationssicher­heit
* Berichten an die Gemeindeschreiberin / den Gemeindeschreiber über zu treffende Informationssicher­heitsmassnahmen und herbeiführen einer Entscheidung
* Beraten der Mitarbeitenden und die Gemeindeschreiberin / den Gemeindeschreiber in Fragen der Infor­mationssicherheit
* Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Infor­mationssicherheit
* Bestimmen der Daten- und Anwendungsverantwortlichen

Anwendungs- und Datenverantwortliche

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

Aufgaben der Anwendungs- und Datenverantwortlichen wahrgenommen:

* Sicherstellen, dass der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu anderen Zwecken nur durch Berechtigte erfolgt
* Bestimmen, wer auf die Anwendung in welcher Form Zugriff hat
* Klassifizieren der Daten, die in ihrem Verantwortungsbereich bearbeitet werden (Vertraulichkeit, Integri­tät, Verfügbarkeit)
* Verantwortung für den sicheren Betrieb ihrer Anwendung (Vertraulichkeit und Integrität der Daten­sammlungen, Verfügbarkeit der Anwendung und Datensammlungen)
* Regeln der Massnahmen für die Informationssicherheit sowie deren Kontrolle und Verantwortung für die Dokumentation der Sicherheitsvorkehrungen
* Kontrollieren der Erfüllung der Datenschutz- und Informationssicherheitsbestimmungen
* Erstellen von Notfallplänen für längere Ausfälle
* Informationsstelle für die in ihrem Verantwortungsbereich liegenden Anwendungen und Datensamm­lungen
* Verantwortung für die Bearbeitung (inklusive Bekannt- und Weitergabe), Archivierung oder Vernichtung der in ihrem Verantwortungsbereich liegenden Daten

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.

Aufgaben der Datenschutzberaterin / des Datenschutzberaters:

* Beraten der Mitarbeitenden und die Gemeindeschreiberin / den Gemeindeschreiber in Fragen des Da­tenschutzes
* Ansprechperson für Betroffene (Auskunfts- und Löschbegehren)
* Berichten an die Gemeindeschreiberin / den Gemeindeschreiber über den Stand des Datenschutzes
* Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Infor­mationssicherheit

## Kontinuierliche Verbesserung der Informationssicherheit

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 wird alle [FRIST VON 1–3 WÄHLEN] Jahre überprüft.

Das Informationssicherheitskonzept 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 die Gemeindeschreiberin / den Gemeindeschreiber mit Beschluss [NR.] am [DATUM]

[ORT UND DATUM] [NAME]

[GEMEINDE] Gemeindeschreiberin / Gemeindeschreiber

V 4.2 / August 2022

Anhang A – Organigramm [GEMEINDE]

Die Informationssicherheitsorganisation der [GEMEINDE] ist gemäss Organigramm vom [DATUM]:

[GRAFIK ORGANIGRAMM MIT DEN PERSONEN UND ZUGEWIESENEN ROLLEN]