Politische Gemeinde Wil ZH

Leitlinie zur Informationssicherheit

vom 19. August 2025

Inhaltsverzeichnis

1 Einleitung 3
2 Geltungsbereich 3
3 Informationssicherheitsniveau 3
4 Informationssicherheitsziele 3
5 Informationssicherheitsmassnahmen 4
6 Informationssicherheitsorganisation 5
6.1. Informationssicherheitsverantwortung 5
6.2. Kontinuierliche Verbesserung der Informationssicherheit 7

1 Einleitung

Die Gemeinde Wil ZH 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 Verarbeitungssystemen nach § 7 Gesetz über die Information und den Datenschutz (IDG, LS 170.4) verabschiedet der Gemeinderat für die Gemeindeverwaltung diese Leitlinie zur Informationssicherheit. Sie trägt zum Datenschutz und zur Informationssicherheit bei, indem sie das von der Gemeinde Wil ZH angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet die Leitlinie eine Beschreibung der Informationssicherheitsorganisation.

2 Geltungsbereich

Die Leitlinie zur Informationssicherheit und die damit zusammenhängenden Dokumente (insbesondere das Rollen-, Berechtigungs- und Schutzbedarfskonzept und die Weisung zur Informationssicherheit) gelten für alle Mitarbeitenden der Gemeindeverwaltung Wil ZH sowie Behördenmitglieder und Funktionäre im Nebenamt. Vertragspartner, die Daten bearbeiten, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

3 Informationssicherheitsniveau

Das Informationssicherheitsniveau der Gemeinde Wil ZH entspricht der «Schutzstufe 1 – Grundschutz» gemäss Allgemeiner Informationssicherheitsrichtlinie AISR der kantonalen Verwaltung. Diese Einstufung erfolgt aufgrund der Tatsache, dass die Anzahl der betroffenen Personen gering 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 Wil ZH bearbeitet auch Daten, die einen erhöhten Schutz vor unberechtigten Zugriffen und von unerlaubten Änderungen benötigen.

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.
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.

5 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.
Physische Sicherheit	Brandschutzmassnahmen usw.

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.

6 Informationssicherheitsorganisation

Die Gemeindeschreiberin / der Gemeindeschreiber und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen haben die zentralen Rollen in der Informationssicherheitsorganisation inne.

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

6.1. Informationssicherheitsverantwortung

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

Gemeindeschreiberin oder Gemeindeschreiber
Die Gemeindeschreiberin oder der Gemeindeschreiber trägt die operative Verantwortung für die Informationssicherheit der Gemeinde Wil ZH. Sie oder er setzt die mit den Informationssicherheitszielen verbundenen Massnahmen um, überwacht die Einhaltung des angestrebten Sicherheitsniveaus, erarbeitet ein Sicherheitskonzept und führt dieses nach.

Die IT- und Anwendungsverantwortlichen sowie die Userinnen und User unterstützen sie oder ihn in ihrer oder seiner Tätigkeit. Sie oder er wird in alle IT-Projekte involviert, um frühzeitig die sicherheitsrelevanten Aspekte einbringen zu können.

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

Aufgaben der oder 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 den Gemeinderat über den Stand der Informationssicherheit
- Beraten der Mitarbeitenden in Fragen der Informationssicherheit
- Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit
- Bestimmen der Anwendungs- und Datenverantwortlichen

<u>Anwendungs- und Datenverantwortliche</u>
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:
- 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

<u>Datenschutzberaterin oder Datenschutzberater</u>
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 oder der Datenschutzberater arbeitet in dieser Rolle eng mit der oder dem Informationssicherheitsverantwortlichen zusammen und ist interne Ansprechperson bei Datenschutzfragen.

Aufgaben der der Datenschutzberaterin oder des Datenschutzberaters:
- Beraten der Mitarbeitenden und der Gemeindeschreiberin oder des Gemeindeschreibers in Fragen des Datenschutzes
- Ansprechperson für Betroffene (Auskunfts- und Löschbegehren)
- Berichten an die Gemeindeschreibern oder den Gemeindeschreiber über den Stand des Datenschutzes
- Planen, koordinieren und umsetzen von Sensibilisierungs- und Schulungsmassnahmen zum Thema Informationssicherheit

6.2. 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 drei Jahre überprüft.

Vom Gemeinderat Wil ZH genehmigt mit Beschluss vom 19. August 2025. Inkraftsetzung per 1. September 2025.

Wil ZH, 19. August 2025 **NAMENS DES GEMEINDERATES**

Urs Rüegg
Gemeindepräsident

Katja Wickihalder
Gemeindeschreiberin