



Politische Gemeinde Wil ZH

Weisung zur Informationssicherheit und zum Datenschutz

vom 19. August 2025

Inhaltsverzeichnis

1	Allgemeine Bestimmungen	3
1.1	Gegenstand und Zweck.....	3
1.2	Geltungsbereich	3
1.3	Grundlagen	3
2	Verantwortung	3
2.1	Verantwortung.....	3
2.2	Mitarbeitende und Behördenmitglieder	3
3	Datenschutz und Informationssicherheit.....	4
3.1	Umgang mit Informationen	4
3.2	Klassifizierung von Informationen	4
3.3	Zugangs- und Zugriffsschutz	5
3.4	Passwörter	6
3.5	Datensicherung, -löschung und Entsorgung von Informationsträgern.....	6
3.6	Virenschutz	6
3.7	Hard- und Software	7
4	Nutzung von E-Mail und Internet.....	7
4.1	Allgemeine Bestimmungen	7
4.2	E-Mail	7
4.3	Internet / Internetdienste.....	7
5	Private Nutzung von IT-Mitteln	8
6	Einsatz mobiler Geräte	8
7	Protokollierung und Kontrolle	9
8	Verwendung von Wechselmedien	9
9	Ausnahmen	9
10	Aufhebung früherer Erlasse	9
11	Genehmigung und Inkrafttreten.....	9

1 Allgemeine Bestimmungen

1.1 Gegenstand und Zweck

Diese Weisung regelt die Nutzung der Informations- und Kommunikationstechnologie (IT-Mittel), im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand der Weisung ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten).

Sie bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

1.2 Geltungsbereich

Die Weisung gilt für alle fest und temporär angestellten Mitarbeitenden sowie für die Behördenmitglieder, welche mit Zugriff auf Applikationen mit hohem Schutzbedarf haben.

1.3 Grundlagen

Die rechtlichen Grundlagen für diese Weisung sind:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)
- Gemeindeordnung der Gemeinde Wil ZH (GO)
- Geschäfts- und Kompetenzreglement des Gemeinderats Wil ZH
- Leitlinie zur Informationssicherheit der Gemeinde Wil ZH vom 19.08.2025
- Rollen-, Berechtigungs- und Schutzbedarfskonzept der Gemeinde Wil ZH vom 19.08.2025

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.

2 Verantwortung

2.1 Verantwortung

Die Gemeindeschreiberin oder der Gemeindeschreiber hat die Rolle als Informationssicherheitsverantwortliche bzw. Informationssicherheitsverantwortlicher (nachfolgend ISV). Sie oder er ist für die Umsetzung dieser Weisung verantwortlich und ist Ansprechstelle für Fragen und für sicherheitsrelevante Vorkommnisse. Sie oder er ist befugt, den Mitarbeitenden Weisungen bezüglich Informationssicherheit zu erteilen.

2.2 Mitarbeitende und Behördenmitglieder

Die Mitarbeitenden der Gemeindeverwaltung sowie die Behördenmitglieder sind verpflichtet, die gesetzlichen Vorgaben, diese Weisung und andere interne Regelungen zu beachten. Sie haben die Kenntnisnahme dieser Weisung unterschriftlich zu bestätigen.

Sie sind verpflichtet, die ihnen zur Verfügung gestellten IT-Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen Personendaten, sorgfältig umzugehen. Alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und Verlust von Hardware und Software sind der oder dem ISV umgehend zu melden.

3 Datenschutz und Informationssicherheit

3.1 Umgang mit Informationen

Informationen sind ausschliesslich gemäss den rechtlichen Vorgaben zu bearbeiten. Im Umgang mit Informationen ist die Vertraulichkeit jederzeit zu gewährleisten. Entsprechende Vorgaben sind jederzeit einzuhalten und entsprechende Massnahmen sicherzustellen. Dazu zählen:

- Informationen nur berechtigten Stellen und Personen zugänglich zu machen;
- Verschlüsseln von sensiblen Informationen bei der Übertragung (beispielsweise Verschlüsselung eines USB-Sticks, einer E-Mail oder einer sonstigen elektronischen Übermittlung);
- Definition von Verfahren, die Informationen und Datenträger während eines physischen Transports schützen;
- Sicherstellen der Vertraulichkeit beim Ausdrucken oder Kopieren von Dokumenten mit Personendaten.

3.2 Klassifizierung von Informationen

Jede physische und elektronische Information ist als "Öffentlich", "Teilweise geheim / Befristet geheim" oder "Geheim" zu klassifizieren. Die Klassifizierung "Geheim" ist gleichzusetzen wie die Klassifizierung "Intern".

Für vertrauliche und geheime Informationen muss ein Klassifizierungsvermerk "Vertraulich" oder "Geheim" angegeben werden. Ist kein Klassifizierungsvermerk vorhanden oder aus dem Kontext erkennbar, gilt die Information als "Intern" klassifiziert.

Wer klassifizierte Informationen bearbeitet, ist für die Einhaltung der Informationsschutzvorschriften verantwortlich.

Wer feststellt, dass Informationen gefährdet, abhandengekommen oder missbraucht worden sind, informiert unverzüglich die beziehungsweise den ISV sowie die zuständige oder vorgesetzte Stelle.

Neu zu erstellende oder anzupassende "Intern", "Vertraulich" oder "Geheim" klassifizierte Dokumente müssen mindestens die folgende Kennzeichnung ausweisen:

- a) Eindeutige Bezeichnung (aussagekräftiger Titel);
- b) Erstellerin / Ersteller, Autorin / Autor oder Dokumenteninhaberin / Dokumenteninhaber;
- c) Funktion des Erstellenden bei "Geheim";
- d) Datum der letzten Überarbeitung;
- e) Klassifizierungsmerkmal bei "Vertraulich" oder "Geheim".

Klassifizierung

- Informationen werden als "Öffentlich" klassifiziert, wenn sie der Öffentlichkeit zugänglich sein dürfen.
- Informationen werden als "Teilweise geheim / Befristet geheim" klassifiziert, der Fall oder das Geschäft noch nicht abgeschlossen ist und nur bestimmte, einzelne Informationen zugänglich sein dürfen bzw. die Informationen nur einem ganz bestimmten Benutzerkreis zur Verfügung gestellt werden können.
- Informationen werden als "Geheim" klassifiziert, wenn Unberechtigte durch deren Kenntnisnahme den Interessen der Wil ZH einen wesentlichen Schaden zufügen könnten.

Schutzmassnahmen für klassifizierte Informationen

Für "**Öffentlich**" klassifizierte Informationen gelten folgende Bearbeitungsregeln:

- Die Integrität der Informationen muss sichergestellt werden.
- Die Informationen sind frei zugänglich bzw. einsehbar.

Für "**Teilweise geheim / Befristet geheim**" klassifizierte Informationen gelten zusätzlich zu den Bearbeitungsregeln für als "Öffentlich" klassifizierte Informationen:

- Informationsträger müssen an einem abschliessbaren Ort aufbewahrt werden.
- Der Zugriff muss beschränkt sein auf einen von der Dateneignerin oder dem Dateneigner namentlich oder funktionsbezogenen definierten Personenkreis.
- Die Weitergabe nach aussen ist nur bei anerkannten Gründen und unter entsprechenden Sicherheitsmassnahmen zulässig (z.B. mit einem Vertrag mit einer Vertraulichkeitsklausel).
- Der elektronische Versand von vertraulichen Dokumenten hat verschlüsselt zu erfolgen.
- Die Informationen sind zum Zeitpunkt der Bearbeitung noch nicht öffentlich, da das Geschäft noch nicht abgeschlossen ist.

Für "**Geheim**" (intern) klassifizierte Informationen gelten zusätzlich zu den Bearbeitungsregeln für als "Teilweise geheim / Befristet geheim" klassifizierte Informationen:

- Jedes Exemplar ist auf jeder Seite als "Geheim" zu kennzeichnen (z.B. mit Wasserzeichen).
- Physische Dokumente müssen an einem stark gesicherten Ort (z.B. Tresor) aufbewahrt werden und stehen somit unter physischer Zugangskontrolle.
- Elektronische Dokumente dürfen nur auf zugelassenen Speicherorten abgelegt werden.
- Die Erstellerin oder der Ersteller führt eine schriftliche Kontrolle über die Ausgabe und den Verbleib der einzelnen nummerierten physischen Dokumente oder bei elektronischen Dokumenten die nummerierten Informationsträger.
- Der Versand muss nachvollziehbar sein.
- Dokumente und elektronischer Versand müssen zusätzlich signiert sein.

3.3 Zugangs- und Zugriffsschutz

Die Mitarbeitenden sorgen dafür, dass keine Unbefugten Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen (z.B. Servicetechniker usw.) in den Büroräumlichkeiten auf, sind Massnahmen zu treffen, die einen unbefugten Zugang zu Informationen verhindern.

Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen von Türen und Verschliessen von Fenstern des Büros, Abschliessen weiterer Räume gemäss Anweisung des ISV, Sperren oder Herunterfahren des Computers). Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen.

Die Mitarbeitenden dürfen nur ihre persönlichen Benutzerkennungen oder die ihnen zugeteilten funktionellen Kennungen verwenden. Sie sind für die mit ihren Kennungen erfolgten Zugriffe verantwortlich. Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten.

Der Verlust von Schlüsseln, Badges, Chipkarten usw. ist umgehend der oder dem ISV zu melden. Besteht der Verdacht, dass Zugangs- oder Zugriffsberechtigungen unberechtigt durch Dritte genutzt werden, ist die oder der ISV umgehend zu informieren.

Austretende Personen haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Gemeindeverwaltung Wil ZH bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder zurückgegeben wurden.

3.4 Passwörter

Passwörter sind vertraulich zu behandeln. Sie sind verschlüsselt zu speichern und vor Unbefugten zu schützen. Dies gilt insbesondere, wenn Passwörter für den persönlichen Gebrauch notiert werden (beispielsweise mit einem Passwortmanager KeePass). Anderen Personen (zum Beispiel Vorgesetzten, IT-Verantwortlichen, ISV usw.) sind Passwörter unter keinen Umständen bekannt zu gegeben. Davon ausgenommen sind Passwörter für die Bewirtschaftung von web-basierten Accounts innerhalb einer Abteilung. Der ISV kann eine Übersicht über die innerhalb einer Abteilung verwendeten, webbasierten Accounts und Passwörter verlangen.

Passwörter müssen gemäss den Anforderungen von Abraxas Secure Connect mindestens zwölf Zeichen lang sein und eine Kombination von mindestens einem Klein- und Grossbuchstaben, einer Ziffer und einem Sonderzeichen enthalten. Leicht zu erratende Passwörter und solche, die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden. Passwörter sollten regelmässig gewechselt werden. Sie sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind. Ein früher bereits benutztes Passwort darf nicht mehr gewählt werden.

Gruppenpasswörter werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind umgehend zu ändern, wenn sich die Zusammensetzung der Gruppe verändert. Gleiches gilt, wenn sie unautorisierten Personen bekannt geworden sind. Initialpasswörter müssen sofort geändert werden.

3.5 Datensicherung, -löschung und Entsorgung von Informationsträgern

Geschäftsbezogene Daten müssen auf Serverlaufwerken gespeichert werden. Die regelmässige Sicherung aller Geschäftsdaten und die sichere Lagerung der dazu benötigten Archivmedien erfolgt durch die Abraxas Informatik AG.

Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden (einfaches Löschen genügt nicht). Nicht mehr benötigte Informationsträger (z.B. USB-Datenträger usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physisch zu vernichten (z.B. Schreddern).

3.6 Virenschutz

Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder ihre Konfiguration verändern. E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind vorsichtig zu behandeln, da sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten. Ihre Anhänge sowie Links auf Websites sollen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort der bzw. dem ISV oder der Abraxas Informatik AG gemeldet werden.

3.7 Hard- und Software

Die Mitarbeitenden dürfen keine Software und keine Hardware-Erweiterungen, insbesondere keine Kommunikationseinrichtungen und externe Massenspeicher installieren bzw. anschliessen. Davon ausgenommen sind USB Sticks. Die Mitarbeitenden dürfen Informatiksysteme, die am Netzwerk angeschlossen sind, nicht gleichzeitig mit einem Netz oder System ausserhalb des internen Netzwerks verbinden (z.B. VPN-Verbindungen).

Nur die oder der IT-Verantwortliche darf Geräte in die Reparatur oder zur Entsorgung geben. Sie oder er stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Gemeindeverwaltung verlassen.

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur durch die zuständige Stelle vorgenommen werden.

4 Nutzung von E-Mail und Internet

4.1 Allgemeine Bestimmungen

E-Mail und Internet werden für die Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Wirtschaftlichkeit, der Datensicherheit und des Datenschutzes eingesetzt. Die Mitarbeitenden haben sich unterschriftlich zur Einhaltung der Nutzungsvorschriften zu verpflichten.

4.2 E-Mail

Externe Internetdienste (z.B. Online-Dateiablagen, Online-Kalender) oder private E-Mail-Systeme dürfen nicht für geschäftliche Zwecke verwendet werden.

E-Mails mit vertraulichem Inhalt (z.B. besondere Personendaten) müssen verschlüsselt versandt werden. Ist eine Verschlüsselung nicht möglich, muss eine andere Versandart gewählt werden.

Das automatische Weiterleiten von E-Mails und das Freigeben der persönlichen Mailbox an eine Drittperson sind nicht erlaubt. Bei Abwesenheiten von mehr als einem Arbeitstag ist die Funktion des Abwesenheitsassistenten zu nutzen.

Das geschäftliche E-Mail-System darf in zurückhaltendem Mass auch für private Zwecke verwendet werden. Das Versenden von E-Mails mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt, mit unnötig grossem Verteiler oder mit der Aufforderung zum Weiterversand im Schneeballsystem ist verboten. Private E-Mails müssen entweder gelöscht oder in einem persönlichen Ordner mit der Bezeichnung "privat" abgelegt werden.

4.3 Internet / Internetdienste

Der Zugriff auf Websites mit rechtswidrigem, pornographischem, rassistischem, sexistischem oder gewaltverherrlichendem Inhalt und der zu privaten Zwecken erfolgende Zugriff auf Chatprogramme, Tauschbörsen und Online-Ticker sind verboten. Das Herunterladen und Installieren von Software aus dem Internet ist nicht gestattet. Die oder der ISV kann das Herunterladen oder die Installation solcher Dateien erlauben.

Geschäftsrelevante Daten dürfen nur mit vorgängigem Einverständnis der Gemeindeschreiberin oder des Gemeindeschreibers im Internet publiziert oder zum Beispiel in Formularen bekannt gegeben werden.

Schützenswerte Informationen und grosse Mengen nicht anonymisierter Personendaten dürfen nur verschlüsselt (z.B. mit https:// oder mittels Webtransfer) über das Internet übermittelt werden.

Die private Nutzung sozialer Netzwerke (Facebook, Instagram usw.) durch IT-Mittel der Gemeindeverwaltung ist nicht erlaubt.

5 Private Nutzung von IT-Mitteln

Die zurückhaltende Benützung von IT-Mitteln für private Zwecke ist grundsätzlich gestattet, soweit dadurch die Systemressourcen wie Speicher und Übertragungskapazität nicht im Übermass belastet werden. Die private Nutzung soll möglichst ausserhalb der Arbeitszeit erfolgen. Während der Arbeitszeit ist sie auf ein Minimum zu beschränken. Geschäftsdaten dürfen nicht privat genutzt oder in privaten Datenablagen gespeichert werden. Private Daten müssen lokal in dem persönlichen Netzwerklaufwerk «H:\» gespeichert werden.

Systemkomponenten und Peripheriegeräte dürfen nicht für private Zwecke vom Arbeitsplatz entfernt werden.

Private Geräte dürfen bei Bedarf für dienstliche Aufgaben eingesetzt werden. Eine direkte Verbindung privater Geräte mit dem produktiven Netzwerk ist untersagt.

6 Einsatz mobiler Geräte

Beim Einsatz mobiler Geräte sind folgende Punkte zu beachten:

- Auf mobilen Geräten (zum Beispiel Notebooks, USB-Datenträger, Smartphones) müssen Dokumente mit vertraulichem bzw. schützenswertem Inhalt (z.B. besondere Personendaten) verschlüsselt gespeichert werden.
- Die Benutzerinnen und Benutzer von mobilen Arbeitsstationen sind selbst für die Datensicherung und die datenschutzgerechte Aufbewahrung verantwortlich.
- Mobile Geräte dürfen in öffentlich zugänglichen Räumen nicht unbeaufsichtigt gelassen werden.
- Die Geräte dürfen nicht Dritten zur Nutzung überlassen werden.
- Der Verlust eines mobilen Gerätes ist unverzüglich der oder dem ISV zu melden.
- Es dürfen auf geschäftlichen Geräten keine zusätzlichen Applikationen installiert werden. Besteht ein begründeter Bedarf, ist die Genehmigung der oder des IT-Verantwortlichen einzuholen.
- Eine Verbindung zu drahtlosen Netzwerken (zum Beispiel WLAN) ist für geschäftliche Zwecke nur zulässig, wenn eine Verschlüsselung eingesetzt wird. Davon ausgenommen ist das WLAN-Netz für das Personal der Gemeindeverwaltung, das bereits besonders geschützt ist.
- Drahtlose Komponenten (zum Beispiel Bluetooth, WLAN, NFC) sind bei Nichtgebrauch zu deaktivieren.
- Die Ortungsdienste sind bei Nichtgebrauch für geschäftliche Zwecke zu deaktivieren.

7 Protokollierung und Kontrolle

Zur Überwachung des richtigen Funktionierens, der Sicherheit, der Integrität und der Verfügbarkeit der Informatik werden Systeme eingesetzt, die Protokolle und Warnmeldungen erzeugen. Internetzugriffe werden aufgezeichnet und ein halbes Jahr gespeichert. Eine personenbezogene Auswertung ist nur nach vorgängiger Information der Benutzerin oder des Benutzers möglich.

Ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und / oder personalrechtliche Konsequenzen haben.

8 Verwendung von Wechselmedien

- Der Einsatz von nicht genehmigten Wechselmedien ist verboten.
- Wechselmedien, die klassifizierte Informationen enthalten, müssen gesichert aufbewahrt werden, um den Datenverlust oder -diebstahl zu vermeiden.
- Verluste von Wechselmedien müssen der bzw. dem ISV gemeldet werden.
- Wechselmedien müssen mit einem Passwortschutz versehen und durch Verschlüsselung geschützt werden.
- Wechselmedien müssen zuerst mit einer anerkannten Methode gelöscht werden, bevor sie zum Einsatz kommen.
- Wechselmedien müssen bei der Entsorgung mit einer anerkannten, sicheren Methode gelöscht oder physisch zerstört werden.
- Eine physische Übergabe von Wechselmedien darf nur an eine autorisierte Person erfolgen und muss protokolliert werden.
- Jede Information, die auf einem Wechselmedium abgelegt ist, muss mindestens auf einem weiteren Medium gesichert sein.

9 Ausnahmen

Die oder der ISV entscheidet über Ausnahmen von der vorliegenden Weisung. Entsprechende Gesuche sind ihr oder ihm mit Begründung per E-Mail einzureichen.

10 Aufhebung früherer Erlasse

Auf den Zeitpunkt des Inkrafttretens dieser Verordnung wird die Weisung zum Öffentlichkeitsgrundsatz vom 26. Juli 2016 aufgehoben und durch diese Weisung ersetzt.

11 Genehmigung und Inkrafttreten

Ein widerrechtliches oder weisungswidriges Verhalten im Umgang mit Datenschutz und Informationssicherheit kann straf-, zivil- und / oder personalrechtliche Konsequenzen haben.

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