Strategisches Dokument · vom Gemeinderat zu erlassen

Leitlinie zur Informationssicherheit

VERSION	BESCHLUSS	IN KRAFT AB	KLASSIFIZIERUNG
1.0	GRB 2027-045 vom 15.02.2027	01.03.2027	öffentlich

VERSION	DATUM	BESCHREIBUNG	NAME
0.1	18.01.2027	Entwurf erstellt	Elchi Studios
1.0	15.02.2027	Vom Gemeinderat beschlossen, GRB 2027-045	Beat Beispiel

1 Zweck

Die Politische Gemeinde Musterwil erfüllt ihre Aufgaben nur mit funktionierenden Informations- und Kommunikationssystemen (IKT). Sie bearbeitet dabei Personendaten der Bevölkerung, darunter besondere Personendaten wie Steuer-, Sozialhilfe- und Gesundheitsangaben.

Gestützt auf § 7 des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4) legt der Gemeinderat mit dieser Leitlinie fest:

- welches Sicherheitsniveau die Gemeinde anstrebt,
- welche Ziele sie mit der Informationssicherheit verfolgt,
- nach welchen Grundsätzen sie ihre Massnahmen ausrichtet,
- wer wofür verantwortlich ist.

Die Leitlinie ist die oberste Vorgabe der Gemeinde zu Informationssicherheit und Datenschutz. Alle weiteren Richtlinien, Weisungen und Konzepte stützen sich auf sie.

2 Geltungsbereich

Die Leitlinie gilt für:

- alle Mitarbeitenden der Gemeindeverwaltung einschliesslich Lernende, Praktikantinnen und Praktikanten sowie temporär Beschäftigte,
- die Mitglieder des Gemeinderats, der Kommissionen und der weiteren Behörden der Gemeinde, soweit sie Informationen der Gemeinde bearbeiten,
- alle Informationen der Gemeinde, unabhängig davon, ob sie elektronisch oder auf Papier vorliegen,
- alle IKT-Mittel, die für die Gemeinde eingesetzt werden, auch wenn Dritte sie betreiben.

Dritte, die im Auftrag der Gemeinde Daten bearbeiten (insbesondere die Muster Informatik AG und die Anbieter von Fachanwendungen), werden vertraglich zur Einhaltung dieser Leitlinie und der darauf gestützten Vorgaben verpflichtet.

3 Angestrebtes Sicherheitsniveau

Der Gemeinderat strebt für die gesamte Verwaltung ein Sicherheitsniveau an, das einem normalen Schutzbedarf angemessen ist. Er orientiert sich dabei an den Minimalanforderungen der Datenschutzbeauftragten des Kantons Zürich für Gemeinden mit weniger als 6000 Einwohnerinnen und Einwohnern (Niveau S1).

Grundlage für diesen Entscheid sind:

- die Grösse der Gemeinde (3'850 Einwohnerinnen und Einwohner, 18 Mitarbeitende),
- die Art der bearbeiteten Daten,
- die Abhängigkeit der Verwaltung von ihren IKT-Systemen,
- der vertretbare personelle und finanzielle Aufwand.

Anwendungen und Datensammlungen mit hohem oder sehr hohem Schutzbedarf, insbesondere solche mit besonderen Personendaten, erhalten zusätzliche Schutzmassnahmen. Welche das sind, ergibt sich aus der Schutzbedarfsanalyse.

4 Ziele

Ziel	Bedeutung für Musterwil
Vertraulichkeit	Informationen sind nur berechtigten Personen zugänglich. Personendaten gelangen nicht unrechtmässig an Dritte.
Integrität	Informationen sind richtig und vollständig. Unbefugte Änderungen werden verhindert oder erkannt.
Verfügbarkeit	Informationen und Systeme stehen zur Verfügung, wenn sie gebraucht werden. Ausfälle beeinträchtigen den Verwaltungsbetrieb nicht wesentlich.
Zurechenbarkeit	Jede Bearbeitung von Informationen lässt sich einer Person zuordnen.
Nachvollziehbarkeit	Änderungen an Informationen sind erkennbar und nachvollziehbar.
Verantwortung	Behörden und Mitarbeitende kennen ihre Verantwortung im Umgang mit Informationen und IKT-Mitteln und handeln danach.

5 Grundsätze

Die Gemeinde wählt ihre technischen und organisatorischen Massnahmen nach anerkannten Standards aus, insbesondere nach dem IT-Grundschutz des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) in der Fassung des Minimummassnahmenkatalogs der Datenschutzbeauftragten. Es gelten folgende Grundsätze:

Bereich	Grundsatz
Organisation	Zuständigkeiten und Stellvertretungen sind festgelegt und dokumentiert. Stellvertretende sind so instruiert, dass sie die Aufgabe übernehmen können.
Datenschutz	Personendaten werden nur rechtmässig, zweckgebunden und verhältnismässig bearbeitet. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung und Löschung sind gewährleistet.
Zugriff	Wer auf welche Daten zugreifen darf, regelt ein Rollen- und Berechtigungskonzept. Es gilt das Prinzip der minimalen Rechte.
Passwörter und Anmeldung	Alle Zugänge sind persönlich und mit starken Passwörtern geschützt. Zugriffe von aussen erfordern eine Zwei-Faktor-Authentisierung.
Sensibilisierung	Alle Mitarbeitenden und Behördenmitglieder werden bei Eintritt und danach mindestens jährlich geschult.
Weisungen	Mitarbeitende halten Gesetze, Verträge und interne Weisungen ein. Sie melden Sicherheitsvorfälle und Schwachstellen sofort.
Aktualisierung	Server, Arbeitsplätze, Netzwerkgeräte und Anwendungen werden regelmässig mit Sicherheitsupdates versorgt.
Schadsoftware und Internet	Alle Systeme sind gegen Schadsoftware geschützt. Die Risiken von E-Mail und Internet werden technisch und organisatorisch gering gehalten.
Netzwerk	Alle Netzzugänge sind gesichert. Die Vorgaben des Kantons für den Anschluss an das kantonale Netz (Leunet) werden eingehalten.
Verschlüsselung	Vertrauliche Informationen und besondere Personendaten werden über öffentliche Netze nur verschlüsselt übertragen und auf mobilen Geräten verschlüsselt gespeichert.
Datensicherung	Daten werden regelmässig gesichert, getrennt vom Produktivsystem aufbewahrt, und die Wiederherstellung wird getestet.
IKT-Systeme	Systeme werden sicher beschafft, eingerichtet, betrieben und ausser Betrieb genommen. Datenträger werden vor der Entsorgung sicher gelöscht.
Mobiles Arbeiten	Telearbeit und der Einsatz mobiler Geräte sind geregelt. Private Geräte werden nur nach ausdrücklicher Regelung zugelassen.
Auslagerung	Werden Datenbearbeitungen an Dritte ausgelagert, regeln schriftliche Verträge Datenschutz, Informationssicherheit und Kontrollrechte.
Überwachung	Verfügbarkeit und sicherheitsrelevante Ereignisse der Systeme werden überwacht und protokolliert.
Physische Sicherheit	Gebäude, Büros und Technikräume sind gegen unbefugten Zutritt, Feuer, Wasser und Stromausfall angemessen geschützt.
Aufbewahrung und Archivierung	Informationen werden nach den gesetzlichen Fristen aufbewahrt, dem Gemeindearchiv Musterwil angeboten oder sicher vernichtet.
Notfälle	Ein Notfallkonzept regelt, wie die Gemeinde bei schweren Störungen und Sicherheitsvorfällen handelt und kommuniziert.

6 Organisation und Verantwortung

6.1 Gemeinderat

Der Gemeinderat trägt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz in der Gemeinde. Er beschliesst diese Leitlinie, stellt die nötigen personellen und finanziellen Mittel bereit und lässt sich mindestens jährlich über den Stand informieren.

6.2 Gemeindeschreiberin oder Gemeindeschreiber

Die Gemeindeschreiberin oder der Gemeindeschreiber trägt die operative Verantwortung. Sie oder er:

- bestimmt die informationssicherheitsverantwortliche Person (ISV) und die Datenschutzberaterin oder den Datenschutzberater samt Stellvertretungen,
- erlässt die Allgemeine Richtlinie, die Technische Richtlinie und die Konzepte, soweit nicht der Gemeinderat zuständig ist,
- sorgt dafür, dass die Beschlüsse des Gemeinderats umgesetzt werden,
- erstattet dem Gemeinderat jährlich Bericht.

6.3 Informationssicherheitsverantwortliche Person (ISV)

Die ISV koordiniert die Informationssicherheit in der Verwaltung. Sie erarbeitet und aktualisiert die Sicherheitsvorgaben, überwacht deren Umsetzung, ist Anlaufstelle für Sicherheitsfragen und Vorfälle und steuert den IKT-Dienstleister in Sicherheitsfragen. In sicherheitsrelevanten Fragen ist sie gegenüber Mitarbeitenden und Dienstleistern weisungsberechtigt. Sie berichtet direkt der Gemeindeschreiberin oder dem Gemeindeschreiber und wird frühzeitig in alle Informatikprojekte einbezogen.

Die ISV erhält dafür ausreichend Zeit und Weiterbildung. Die Funktion wird weder von der Gemeindeschreiberin oder dem Gemeindeschreiber noch vom IKT-Dienstleister wahrgenommen, damit Umsetzung und Kontrolle getrennt bleiben.

6.4 Datenschutzberaterin oder Datenschutzberater

Die Datenschutzberatung berät Verwaltung und Behörden in Datenschutzfragen, bearbeitet Auskunfts- und Löschbegehren, ist Ansprechstelle für die kantonale Datenschutzbeauftragte und sorgt für die Meldung von Datenschutzvorfällen. Sie arbeitet eng mit der ISV zusammen.

6.5 Anwendungs- und Datenverantwortliche

Für jede Fachanwendung und Datensammlung ist eine verantwortliche Person bestimmt, in der Regel die zuständige Abteilungsleitung. Sie legt den Schutzbedarf fest, entscheidet über Zugriffsberechtigungen und ist für die rechtmässige Bearbeitung, Aufbewahrung und Löschung der Daten verantwortlich.

6.6 Mitarbeitende und Behördenmitglieder

Alle Mitarbeitenden und Behördenmitglieder tragen mit sicherheitsbewusstem Verhalten zur Informationssicherheit bei. Sie halten die Weisungen ein, nehmen an Schulungen teil und melden Vorfälle, Verdachtsfälle und Schwachstellen unverzüglich der ISV.

7 Dokumente der Informationssicherheit

Die Leitlinie wird durch folgende Dokumente konkretisiert:

Ebene	Dokument	Erlassen durch
Strategisch	Leitlinie zur Informationssicherheit	Gemeinderat
Taktisch	Allgemeine Richtlinie für Informationssicherheit und Datenschutz	Gemeindeschreiber/in und/oder Gemeinderat
Taktisch	Technische Richtlinie für den Betrieb von Informationssystemen	Gemeindeschreiber/in
Operativ	Weisung zur Informationssicherheit und zum Datenschutz	Gemeinderat
Operativ	Erklärung über die Nutzung von Internet und E-Mail	unterzeichnet von allen Mitarbeitenden
Operativ	Rollen- und Berechtigungskonzept, Sensibilisierungskonzept, Notfallkonzept, Betriebsdokumentation	Gemeindeschreiber/in bzw. ISV
Analyse	Schutzbedarfsanalyse, Bedrohungsanalyse, Massnahmenkatalog	ISV, genehmigt durch Gemeindeschreiber/in

8 Überprüfung und Verbesserung

Der Gemeinderat überprüft diese Leitlinie alle 2 Jahre sowie bei wesentlichen Änderungen der Rechtslage oder der Organisation.

Die Umsetzung der Massnahmen wird jährlich sowie bei Projekten mit grossen Auswirkungen auf Informationssicherheit oder Datenschutz auf Aktualität und Wirksamkeit geprüft. Festgestellte Mängel werden innert angemessener Frist behoben. Die Massnahmen orientieren sich am Stand der Technik.

9 Inkrafttreten

Diese Leitlinie wurde vom Gemeinderat mit Beschluss Nr. 2027-045 vom 15. Februar 2027 erlassen und tritt am 1. März 2027 in Kraft.

Musterwil, 15. Februar 2027

Namens des Gemeinderats

GEMEINDEPRÄSIDENTIN

Anna Muster

GEMEINDESCHREIBER

Beat Beispiel

Beilage: Antrag und Beschluss des Gemeinderats

Gremium	**Gemeinderat Musterwil**
Sitzung	**15. Februar 2027**
Beschluss Nr.	**2027-045**
Registratur	**0.4.1 Informatik, Datenschutz**

Informationssicherheit und Datenschutz: Erlass der Leitlinie zur Informationssicherheit und der Weisung zur Informationssicherheit und zum Datenschutz

Ausgangslage

Die Gemeindeverwaltung ist für nahezu alle Aufgaben auf Informatikmittel angewiesen. Sie bearbeitet dabei Personendaten der Bevölkerung, darunter besondere Personendaten in den Bereichen Steuern, Soziales und Einwohnerkontrolle. Cyberangriffe auf Gemeinden in der Schweiz haben in den letzten Jahren zugenommen.

Nach § 7 IDG muss die Gemeinde Informationen durch angemessene organisatorische und technische Massnahmen schützen. Die Datenschutzbeauftragte des Kantons Zürich überprüft dies mit dem Datenschutzreview. Gemeinden reichen dabei eine Selbstdeklaration mit den erforderlichen Dokumenten ein. Die Datenschutzbeauftragte stellt ihren Bericht der Gemeinde und dem Bezirksrat Affoltern zu.

Die Gemeinde hat nach der Einladung der Datenschutzbeauftragten vom 12. Oktober 2026 die erforderlichen Dokumente erarbeiten lassen.

Erwägungen

Die Leitlinie ist das oberste Dokument der Informationssicherheit. Sie legt Sicherheitsniveau, Ziele, Grundsätze und Verantwortlichkeiten fest und muss vom Gemeinderat erlassen werden. Die Weisung regelt verbindlich, wie Mitarbeitende und Behördenmitglieder mit Informationen und Informatikmitteln umgehen.

Der Gemeinderat strebt ein Sicherheitsniveau für normalen Schutzbedarf an. Das entspricht den Minimalanforderungen der Datenschutzbeauftragten für Gemeinden unter 6000 Einwohnerinnen und Einwohnern. Für besonders schützenswerte Daten werden zusätzliche Massnahmen getroffen.

Die operative Verantwortung liegt beim Gemeindeschreiber. Damit Umsetzung und Kontrolle getrennt bleiben, wird die Funktion der informationssicherheitsverantwortlichen Person einer anderen Person übertragen.

Beschluss

Der Gemeinderat beschliesst:

1. Die Leitlinie zur Informationssicherheit der Politischen Gemeinde Musterwil wird erlassen und tritt am 1. März 2027 in Kraft.
2. Die Weisung zur Informationssicherheit und zum Datenschutz wird erlassen und tritt am 1. März 2027 in Kraft.
3. Die Allgemeine Richtlinie für Informationssicherheit und Datenschutz wird genehmigt.
4. Der Gemeinderat nimmt Kenntnis davon, dass der Gemeindeschreiber folgende Personen bestimmt hat: informationssicherheitsverantwortliche Person Daniel Platzhalter, Leiter Finanzen (Stellvertretung Eva Entwurf); Datenschutzberaterin Franziska Muster, Einwohnerdienste.

5. Der Gemeindeschreiber wird beauftragt, die Selbstdeklaration mit den erforderlichen Dokumenten bei der Datenschutzbeauftragten einzureichen und dem Gemeinderat jährlich über den Stand der Informationssicherheit Bericht zu erstatten.
6. Die Mitarbeitenden werden über die Leitlinie und die Weisung informiert, geschult und unterzeichnen die Erklärung über die Nutzung von Internet und E-Mail.
7. Dieser Beschluss ist öffentlich. Die Leitlinie und die Weisung werden in die Rechtssammlung der Gemeinde aufgenommen.
8. Mitteilung an: Gemeindeschreiber; informationssicherheitsverantwortliche Person; Datenschutzberaterin; Abteilungsleitungen; Muster Informatik AG (Auszug, zur Kenntnis); Akten.

Gemeinderat Musterwil

GEMEINDEPRÄSIDENTIN	GEMEINDESCHREIBER
Anna Muster	**Beat Beispiel**