

**Gemeinderat**



## **ICT-Sicherheitsleitlinien**

vom 22. November 2021

## Inhaltsverzeichnis

	<b>Seite</b>
Art. 1 Einleitung	3
Art. 2 Geltungsbereich	3
Art. 3 Informationssicherheitsniveau	3
Art. 4 Informationssicherheitsziele	4
Art. 5 Massnahmen	4/5
Art. 6 Informationssicherheitsverantwortung, Grundsatz	5
Art. 7 Informationssicherheitsverantwortung	6
Art. 8 Kontinuierliche Verbesserung der Informationssicherheit	6
Art. 9 Inkrafttreten	7

**Art. 1**

Die Gemeindeverwaltung Geroldswil ist zur Aufgabenerfüllung von zuverlässig funktionierenden Systemen der Informations- und Kommunikationstechnologie (ICT-Systeme) abhängig. Zur Gewährleistung der Integrität, Vertraulichkeit, Verfügbarkeit, Nachvollziehbarkeit und Authentizität der Informationen und deren Verarbeitungssysteme nach § 7 Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007 verabschiedet der Gemeinderat diese Leitlinie zur Informationssicherheit (ICT-Sicherheitsleitlinie). Sie trägt zum sicheren Betrieb und zur sicheren Nutzung der ICT bei, indem sie das von der Gemeindeverwaltung angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet diese Leitlinie eine kurze Beschreibung der Informationssicherheitsorganisation.

Einleitung

Entsprechend dem Grundsatz der Gleichberechtigung von Mann und Frau gelten alle Personen- und Funktionsbezeichnungen dieser Sicherheitsleitlinie, ungeachtet der männlichen oder weiblichen Sprachform, für beide Geschlechter.

**Art. 2**

Diese ICT-Sicherheitsleitlinie und die damit zusammenhängenden Dokumente gelten für alle Nutzer der ICT-Infrastruktur der Politischen Gemeinde Geroldswil. Vertragspartner, welche Dienstleistungen im Bereich ICT erbringen, werden zur Einhaltung der im Folgenden aufgeführten Anforderungen verpflichtet.

Geltungsbereich

**Art. 3**

Das Informationssicherheitsniveau der Gemeindeverwaltung wird als "mittel" eingestuft. Dies entspricht der Sicherheitsstufe 2 nach § 12 Abs. 1 der Verordnung über die Informationsverwaltung und -sicherheit (IVSV) vom 3. September 2019 sowie 5.9 a) der Allgemeinen Informationssicherheitsrichtlinie des Regierungsrates des Kantons Zürich vom 3. September 2019. Diese Einstufung erfolgt aufgrund der Tatsache, dass alle wesentlichen Funktionen und Aufgaben durch ICT-Systeme unterstützt werden und ein Ausfall von ICT-Systemen die Aufgabenerfüllung nicht beeinträchtigen darf. Als öffentliche Verwaltung bearbeitet die Gemeindeverwaltung auch Daten, welche einen erhöhten Schutz vor unberechtigten Zugriffen und von unerlaubten Änderungen benötigen.

Informations-  
sicherheitsniveau

#### **Art. 4**

Aus der Einstufung ergeben sich die folgenden Informationssicherheitsziele (§ 7 IDG vom 12. Februar 2007):

Informationssicherheitsziele

Vertraulichkeit:

Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.

Integrität:

Informationen müssen richtig und vollständig sein.

Authentizität:

Informationsbearbeitungen müssen einer Person zugeordnet werden können.

Nachvollziehbarkeit:

Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

#### **Art. 5**

Aus der Definition der Informationssicherheitsziele ergeben sich folgende Massnahmen:

Massnahmen

Passwörter:

Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch personenabhängige Passwörter gesichert.

Berechtigungskonzept:

Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben geeignet und erforderlich.

Backup:

Die Datensicherung wird regelmässig durchgeführt. Die Sicherungsmedien werden an getrennten Orten aufbewahrt und sind physisch geschützt. Es wird gewährleistet, dass kurzfristig verlorene oder fehlerhafte Teile des Informationsbestandes wiederhergestellt werden können.

Virenschutz / Internet:

Viren-Schutzprogramme werden auf allen ICT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.

Mobile Geräte / Software:

Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten sowie die Installation von Software auf Arbeitsplatzrechnern und Servern sind geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.

Zutritt:

Gebäude und Räume sowie ICT-Systeme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.

Verschlüsselung:

Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotentials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, wie z. B. von besonderen Personendaten, erfolgt über öffentliche Netze verschlüsselt.

Monitoring:

Die Verfügbarkeit und Qualität von Internet-Diensten für Bürgerinnen und Bürger wird laufend überprüft.

Weisungen:

Die ICT-Nutzer werden angewiesen, die Gesetze sowie die vertraglichen Regelungen und internen Richtlinien einzuhalten. Sie unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmassnahmen. ICT-Sicherheitsfragen und Hinweise auf Schwachstellen sind an den ICT-Verantwortlichen zu richten.

Organisation:

Für alle Funktionen wird die Stellvertretung geregelt. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe erfüllen können.

Sensibilisierung:

Die ICT-Nutzer nehmen an den internen Sicherheitsschulungen teil, welche vom ICT-Administrator durchgeführt werden. Sie werden über aktuelle Gefahren und zu treffende Massnahmen informiert.

Firewall:

Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern. Die Network Security Police der übergeordneten Netzwerke wird eingehalten.

**Art. 6**

Die zentralen Rollen in der Informationssicherheitsorganisation haben der Gemeindeschreiber, der ICT-Verantwortliche und die für die einzelnen Bereiche zuständigen Daten- und Anwendungsverantwortlichen inne.

Informations-  
sicherheits-  
verantwortung,  
Grundsatz

### **Art. 7**

Der Gemeindegeschreiber trägt die Gesamtverantwortung für die Informationssicherheit in der Politischen Gemeinde Geroldswil.

Informationssicherheitsverantwortung

Zur Umsetzung der Informationssicherheitsziele und Überwachung der Einhaltung des angestrebten Sicherheitsniveaus ist der ICT-Verantwortliche zuständig. Dieser ist für die Ausarbeitung und Nachführung einer ICT-Weisung verantwortlich. Er berichtet in dieser Funktion direkt dem Gemeindegeschreiber, welcher die Weisung erlässt.

Die ICT-Daten- und Anwendungsverantwortlichen sowie die ICT-Nutzer unterstützen den ICT-Verantwortlichen in seiner Tätigkeit. Er wird in alle ICT-Projekte involviert, um frühzeitig die notwendigen sicherheitsrelevanten Aspekte einbringen zu können.

Für sicherheitsrelevante Fragen ist der ICT-Verantwortliche weisungsberechtigt. Er ist die Anlaufstelle für Informationssicherheitsfragen und Hinweise auf Schwachstellen.

Der ICT-Verantwortliche verfügt über ein angemessenes Wissen sowie entsprechende Fähigkeiten. Für alle Prozesse, Daten, ICT-Anwendungen und ICT-Systeme kann von ihm eine verantwortliche Person benannt werden, die den jeweiligen Schutzbedarf (Klassifizierung) bestimmt und die Zugriffsberechtigungen vergibt.

### **Art. 8**

Der Gemeinderat unterstützt die Einhaltung und weitere Verbesserung des Informationssicherheitsniveaus. Er gibt mit der periodischen Überarbeitung dieser ICT-Sicherheitsleitlinie die notwendigen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung. Sie wird mindestens einmal pro Amtsdauer überprüft.

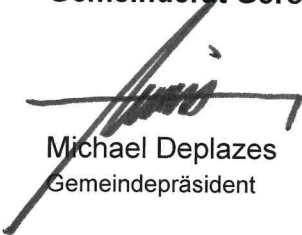
Kontinuierliche Verbesserung der Informationssicherheit

Die ICT-Weisung wird regelmässig auf Aktualität und Wirksamkeit geprüft. Festgestellte Abweichungen werden innert nützlicher Frist behoben. Die zu ergreifenden Massnahmen orientieren sich an der ICT-Sicherheitsleitlinie und am Stand der Technik sowie an nationalen und internationalen Standards.

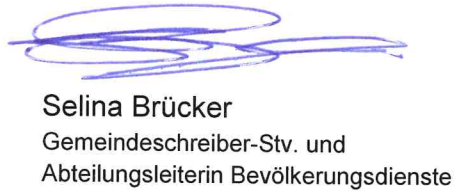
**Art. 9**

Diese ICT-Sicherheitsleitlinie tritt per 1. Januar 2022 in Kraft. Gleichzeitig Inkrafttreten  
werden alle im Widerspruch zu dieser ICT-Sicherheitsleitlinie stehenden  
kommunalen Erlasse und Beschlüsse aufgehoben.

**Gemeinderat Geroldswil**



Michael Deplazes  
Gemeindepräsident



Selina Brücker  
Gemeindeschreiber-Stv. und  
Abteilungsleiterin Bevölkerungsdienste