dsb
datenschutzbeauftragte
des kantons zürich

Vorlage

# Rollen- und Berechtigungskonzept Gemeinde X

**Erläuterung zur Vorlage**
Das vorliegende Dokument Rollen- und Berechtigungskonzept 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 publiziert.

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

## Inhalt

# 1 Gegenstand und Zweck

Das Rollen- und Berechtigungskonzept dient dem Schutz der Vertraulichkeit und der Integrität. Dieses Dokument ist die Grundlage für die [GEMEINDE] zur Implementierung der Berechtigungen.

Ziele des Rollen- und Berechtigungskonzepts sind:
- Klarheit bei der Vergabe von Rechten
- Übergreifende, verbindliche Definition der Berechtigungsvergabe
- Verringerung des administrativen Aufwands

# 2 Geltungsbereich

Dieses Rollen- und Berechtigungskonzept gilt für alle Mitarbeitenden der [GEMEINDE]. Die Auftragnehmenden im IT-Bereich werden zur Einhaltung der entsprechenden Anforderungen vertraglich verpflichtet.

# 3 Konzeptionelle Vorgaben

## 3.1 Verantwortung

Damit die Informationssicherheit sinnvoll umgesetzt werden kann, wird die Verantwortung auf verschiedene Verantwortungsträgerinnen und -träger verteilt (Ownership-Prinzip). Die Hauptverantwortung für die Informationssicherheit liegt bei der Gemeindeschreiberin / dem Gemeindeschreiber. Sie respektive er delegiert die Aufgaben und Kompetenzen an die Daten- und Anwendungsverantwortlichen und/oder an die IT-Verantwortliche / den IT-Verantwortlichen.

## 3.2 Grundlagen

Folgende Grundlagen und Dokumente enthalten Aspekte der Verantwortlichkeit:
- Gemeindeordnung vom [DATUM]
- Geschäftsordnung des Gemeinderates vom [DATUM]
- Leitlinie zur Informationssicherheit vom [DATUM]
- Stellenbeschreibung der Mitarbeitenden

## 3.3 Risikobeurteilung und Sicherheitsstufe

Die Zuordnung der Informationen erfolgt aufgrund der Risikoanalyse in die vom Regierungsrat festgelegten Schutzstufen nach der Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8). Alle Systeme, Anwendungen und Informationen der [GEMEINDE] werden in diesem Konzept berücksichtigt.

## 3.4 Prozesse

Es ist ein Prozess einzurichten, der den Antrag und die Vergabe von Berechtigungen nachvollziehbar und vollständig aufzeichnet.

Die Berechtigungen für den Zugriff auf IT-Systeme und Anwendungen werden durch die verantwortlichen Personen gemäss Zugriffsmatrix geprüft, genehmigt und regelmässig kontrolliert.

### 3.5 Zugriffskontrolle

Alle eingesetzten IT-Systeme (Zentralsysteme, Endbenutzersysteme wie PC, Terminalserverclients usw.) sind durch Zugriffskontrolle vor unerlaubter Nutzung zu schützen. Jeder Anwender und jede Anwenderin wird mindestens durch eine Identifikation und ein Passwort gegenüber dem System identifiziert und authentifiziert.

Der Auftragnehmende in der Funktion Netzwerkadministrator unterhält und betreibt die Netzwerkkomponenten und die Abtrennung des internen Netzwerks von Fremdnetzen (Firewall). Er dokumentiert die Gemeinde mit den notwendigen Unterlagen (Grundsätze, Filterregeln mit zugelassenen Verbindungen, Umfang, Empfängerkreis und Periodizität der Auswertungen und Meldungen).

### 3.6 Support

Für Supportaufgaben kann der Auftragnehmende auf die Systeme zugreifen. Der Zugriff findet unter Beaufsichtigung durch die Benutzerin oder den Benutzer statt.

## 4 Funktionen

### 4.1 Funktionen innerhalb der Gemeinde

Gemäss Organigramm vom [DATUM]:
[GRAFIK ORGANIGRAMM MIT DEN PERSONEN UND ZUGEWIESENEN ROLLEN]

Hinweis: Werden mehrere Funktionen durch dieselben Mitarbeitenden wahrgenommen, so sind mögliche Interessenkonflikte durch unterschiedliche Rollen zu verhindern (Segregation of Duties).

### 4.2 Funktionen im IT-Bereich

Die nachfolgenden Funktionen werden durch die IT-Verantwortliche respektive den IT-Verantwortlichen wahrgenommen. Davon ausgenommen ist der Bereich der Revision und bei einer Auslagerung die Rolle der Administratoren, die von der Auftragnehmerin [FIRMA] wahrgenommen wird.

**IT-Sicherheitsverantwortliche / IT-Sicherheitsverantwortlicher**

Die oder der IT-Sicherheitsverantwortliche überwacht alle getroffenen IT-Massnahmen der externen Auftragnehmenden und prüft regelmässig die Einhaltung der Sicherheitszielsetzungen. Sie oder er setzt die Verordnung über die Informationsverwaltung und -sicherheit um und regelt den Ablauf der regelmässigen Prüfung gemäss § 14 IVSV, plant die Sensibilisierung und Schulung für die IT-Sicherheit und führt diese zusammen mit den Daten- und Anwendungsverantwortlichen durch. Sie oder er ist Anlauf- und Meldestelle bei Problemen und Beobachtungen im Bereich IT-Sicherheit und rapportiert an die [VORGESETZTE STELLE] sowie den Daten- und Anwendungsverantwortlichen.

**IT-Verantwortliche / IT-Verantwortlicher**

Die oder der IT-Verantwortliche betreut die IT-Infrastruktur der [GEMEINDE].

**Administratorin / Administrator – Netzwerk und Systeme**

Die Administratorin oder der Administrator unterhält und betreibt die Netzwerkkomponenten (Router, Switches, Firewall), die Server- und Client-Basissysteme (Betriebssystem und betriebssystemnahe Software), E-Mail-Systeme und Büroautomationsprogramme.

**Administratorin / Administrator – Anwendungen und Datenbanken**
Die Administratorin oder der Administrator vergibt alle applikationsbezogenen Rechte (Zugriffe auf Daten, Prozesse wie Masken und Reports sowie Drucker usw.) und Anmeldedefinitionen (Benutzer-ID und Passwort). Sie oder er betreibt und unterhält die Datenbanksysteme in technischer Hinsicht.

**Revision**
Unabhängige Stellen prüfen gemäss § 14 IVSV die rechtlichen, organisatorischen und technischen Massnahmen im IT-Bereich auf der Basis der IVSV und der Leitlinie zur Informationssicherheit respektive dem Informationssicherheitskonzept.

## 5 Zugriffsmatrix

Die Zuweisung der Zugriffsrechte im Dateisystem und in den Anwendungen erfolgt über die Gruppen an Stellen oder Personen.

**Tabelle 1 – Zugriffsmatrix am Beispiel einer Gemeinde [DATEISYSTEM]**

| Gruppenbezeichnung | Funktionen / Zugriff | Gruppenmitglieder | Genehmigung durch |
|---|---|---|---|
| LG_Gemeindeschreiber/in | … | … | … |
| LG_Gemeinderat_w | … | … | … |
| LG_Kanzlei_w | … | … | … |
| LG_Personal_w | … | … | … |
| LG_Informatik_w | … | … | … |
| LG_Internet_w | … | … | … |
| LG_Einwohnerkontrolle_w | … | … | … |
| LG_Hochbau_w | … | … | … |
| LG_Umwelt_w | … | … | … |
| LG_Tiefbau_w | … | … | … |
| LG_Werkhof_w | … | … | … |
| LG_Sicherheit_w | … | … | … |
| LG_Finanzen_w | … | … | … |
| LG_Steuern_w | … | … | … |
| LG_Liegenschaften_w | … | … | … |
| LG_Soziales_w | … | … | … |
| LG_Sozialversicherungen_w | … | … | … |
| LG_Fuersorge_w | … | … | … |
| LG_Vormundschaft_w | … | … | … |
| LG_Bestattungen_w | … | … | … |
| LG_Schulverwaltung_w | … | … | … |
| LG_Schulleitung_w | … | … | … |
| … | … | … | … |

LG = Lokale Gruppe

**Tabelle 2 – Zugriffsmatrix am Beispiel einer Gemeinde [APPLIKATIONEN]**

| Rollenbezeichnung | Beschreibung | Funktionen /Zugriff | Mitglieder der Rolle | Genehmigung durch |
|---|---|---|---|---|
| Baupro | … | Administrator/-in<br>Geschäfte erfassen<br>… | …<br>…<br>… | … |
| Abacus (Finanzbuchhaltung) | | Administrator/-in<br>Rechnungen ausstellen<br>Rechnungen genehmigen | …<br>…<br>… | … |
| Abacus (Lohn) | … | Administrator/-in<br>Lohn ändern<br>… | …<br>…<br>… | … |
| NEST (Einwohnerkontrolle) | … | Administrator/-in<br>Einwohner mutieren<br>… | …<br>…<br>… | … |
| NEST (Steuern) | … | Administrator/-in<br>Steuerausweis drucken | …<br>…<br>… | … |
| Scolaris | … | … | …<br>…<br>… | … |
| Internet (CMS, backslash) | … | … | …<br>… | … |
| Extranet (DMS3, backslash) | … | … | …<br>…<br>… | … |
| Exchange | … | … | … | … |
| … | … | … | … | … |

# 6 Einrichten / Ändern / Löschen der Zugriffsrechte und des Passworts

Die Personalverantwortlichen melden den IT-Verantwortlichen die Anforderungen. Beim erstmaligen Einrichten der Berechtigungen wird ein Initialpasswort durch die IT-Verantwortlichen definiert. Für die Benutzer- und Gruppennamen wird eine Namenskonvention eingehalten.

## 6.1 Verantwortlichkeiten

Die Daten- und Anwendungsverantwortlichen erstellen folgende Aufträge:

- Anpassen der Zugriffsmatrix (Zugriffsberechtigungen für Gruppen)
- Erstellen von Ausnahmebewilligungen (Zugriffsberechtigungen für Mitarbeitende ausserhalb der Zugriffsmatrix)
- Zuweisen von Personen zu Gruppen (Ein-, Über-, Austritt)
- Regelmässiges Überprüfen der eingerichteten Zugriffe auf Richtigkeit und Zweckmässigkeit (falls nötig Einleiten von Korrekturmassnahmen)
- Setzen des Initialpassworts
- Zurücksetzen des Passworts
- Bearbeitung aller Fragen und Probleme rund um Zugriffe und Passwörter

Die Aufträge zur Berechtigungsvergabe sind schriftlich zu formulieren und von der Empfängerin oder dem Empfänger zu visieren. Die eingerichteten Zugriffsdefinitionen werden periodisch auf ihre Richtigkeit und Zweckmässigkeit durch die Daten- und Anwendungsverantwortlichen in Zusammenarbeit mit den IT-Verantwortlichen überprüft.

Die Aufträge werden von den Administratorinnen und Administratoren sorgfältig ausgeführt und die Durchführung wird schriftlich bestätigt. Die oder der IT-Verantwortliche sorgt für die korrekte und vollständige Ablage der Aufträge (Nachvollziehbarkeit).

## 6.2 Prozesse

### Standard

| | |
|---|---|
| Prozess: | Daten- und Anwendungsverantwortliche → IT-Verantwortliche / IT-Verantwortlicher |
| Medium: | Auftrag per [TICKET / MAIL], Rückmeldung per [TICKET / MAIL] |
| Authentifizierung: | Persönlich bekannt, ansonsten Ausweis |
| Initialpasswort: | Durch Daten- und Anwendungsverantwortliche definiert |

### Windows Active Directory (Dateiserver)

| | |
|---|---|
| Prozess: | Personal → Daten- und Anwendungsverantwortliche → IT-Verantwortliche / IT-Verantwortlicher |
| Medium: | Auftrag per [TICKET / MAIL], Rückmeldung per [TICKET / MAIL] |
| Authentifizierung: | Persönlich bekannt, ansonsten Ausweis |
| Initialpasswort: | Durch die IT-Verantwortliche / IT-Verantwortlicher definiert |

## 6.3 Meldestelle bei Problemen mit dem Passwort

Bei Fragen und Problemen bezüglich Passwörter gibt die oder der entsprechende IT-Verantwortliche Auskunft.

# 7 Weitere Massnahmen

## 7.1 Authentifikation der Benutzenden

Grundsätzlich werden alle Benutzenden auf dem Netzwerk und in den Applikationen authentisiert. Andere Benutzende, zum Beispiel technisch bedingte Benutzer-IDs, werden durch [VERANTWORTLICHE PERSON] vergeben, dokumentiert und überwacht.

## 7.2 Dokumentation für Applikationen

Grundsätze zur Rechtevergabe und Massnahmen zur Bewahrung der Integrität (zum Beispiel Logging) sind in den Betriebshandbüchern der Applikationen zu finden.

## 7.3 Lokale Netze, Fremdnetze und Internet

[FIRMA / AUFTRAGNEHMERIN] in der Funktion Netzwerkadministrator unterhält und betreibt die Netzwerkkomponenten und die Abtrennung des internen Netzwerks von Fremdnetzen (Firewall). Sie informiert und dokumentiert betreffend der notwendigen Unterlagen (Grundsätze, Filterregeln mit zugelassenen Verbindungen, Umfang, Empfängerkreis und Periodizität der Auswertungen und Meldungen, zu treffende Massnahmen je nach Bedrohung respektive Vorfall, Vorgehen und Nachweis der Aktualisierungen).

## 7.4 Lokale Administration auf dem Client, Fernzugriff

Die lokale Administration auf dem Client wird durch die IT-Verantwortlichen durchgeführt. Die technische Administration wird durch Mitarbeitende [FIRMA / AUFTRAGNEHMENDE] durchgeführt. Diese können von extern auf die Systeme zugreifen. Die oder der Benutzende muss den Zugriff vorgängig bestätigen. Im Bereich der Hauptapplikationen ([ANWENDUNGEN]) wird die technische Administration durch [FIRMA / AUFTRAGNEHMENDE] durchgeführt.

## 8 Überprüfung der Ein- und Zugriffe

Die Überprüfung der eingerichteten Zugriffe (periodische Nachprüfung der Zugriffsmatrix und der Ausnahmebewilligungen) erfolgt mindestens einmal jährlich durch den IT-Verantwortlichen oder die IT-Verantwortliche und die Daten- und Anwendungsverantwortlichen. Die entsprechende Protokollierung innerhalb der Applikationen und Systeme wird durch die Daten- und Anwendungsverantwortlichen sichergestellt.

Der Zustand, die Resultate und die notwendigen Massnahmen werden schriftlich an die Gemeindeschreiberin oder den Gemeindeschreiber gemeldet.

Vorgehen bei Massnahmen betreffend Zugriffsverletzungen bei sensitiven Daten:

- Die oder der Informationssicherheitsverantwortliche informiert bei besonderen Vorfällen (Zugriffsverletzungen, Integritätsproblemen mit Daten usw.) die Daten- und Anwendungsverantwortlichen der sensitiven Daten. Diese treffen in Absprache mit der Gemeindeschreiberin oder dem Gemeindeschreiber und der oder dem IT-Verantwortlichen die notwendigen Massnahmen zu Bewahrung der Vertraulichkeit und der Integrität.
- Zugriffsverletzungen an den Netzwerkgrenzen und an den Systemen werden aufgezeichnet und in Zusammenarbeit mit den Auftragnehmenden ausgewertet.

Bei folgenden Vorfällen erfolgt eine sofortige Eskalation und Rapportierung an die Gemeindeschreiberin oder den Gemeindeschreiber durch die Informationssicherheitsverantwortliche oder den Informationsverantwortlichen.

- Firewall-Funktionalität nicht mehr vorhanden oder gestört
- Serverfunktionalität nicht mehr vorhanden oder gestört
- Zugriffsmatrix nicht eingehalten oder Einhaltung zweifelhaft
- Mehr als 100 abgewiesene Zugriffe innerhalb 1 Stunde (Netzwerk / Server)
- Integrität der Daten einer Hauptanwendung nicht mehr gegeben oder zweifelhaft
- Mehr als 100 abgewiesene Zugriffe innerhalb 1 Stunde bei den sensitiven Daten

V 5.2 / November2022