Vorlage

Rollen- und Berechtigungskonzept [Gemeinde/Stadt]

Erläuterung zur Vorlage

Die Vorlage 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 beziehungsweise > 6000 zu entnehmen.

Die Vorlage ist den jeweiligen Gegebenheiten anzupassen. Die anzupassenden Punkte befinden sich in eckigen Klammern [ ].

Der Leitfaden Informationssicherheit in Gemeinden, die Vorlagen und weitere Dokumente sind auf [www.datenschutz.ch](https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/informationssicherheit) publiziert.

Änderungskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung, Bemerkung | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhalt

[1 Allgemeine Bestimmungen 3](#_Toc180397383)

[1.1 Gegenstand und Zweck 3](#_Toc180397384)

[1.2 Geltungsbereich 3](#_Toc180397385)

[1.3 Grundlagen 3](#_Toc180397386)

[2 Konzeptionelle Vorgaben 3](#_Toc180397387)

[2.1 Zugriffskontrolle 3](#_Toc180397388)

[2.2 Zugriffsrechte 3](#_Toc180397389)

[2.3 Prozesse 3](#_Toc180397390)

[2.4 Support 4](#_Toc180397391)

[2.5 Authentifikation der Benutzerinnen und Benutzer 4](#_Toc180397392)

[3 Funktionsrollen 4](#_Toc180397393)

[4 Berechtigungen 5](#_Toc180397394)

[5 Verantwortlichkeiten und Prozesse 6](#_Toc180397395)

[5.1 Verantwortlichkeiten 6](#_Toc180397396)

[5.2 Prozess Einrichten / Ändern von Zugriffsberechtigungen 7](#_Toc180397397)

[5.3 Löschen von Zugriffsberechtigungen 7](#_Toc180397398)

[5.4 Einrichten / Zurücksetzen des Passworts 7](#_Toc180397399)

[6 Genehmigung und Inkrafttreten 7](#_Toc180397400)

# Allgemeine Bestimmungen

## Gegenstand und Zweck

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

Ziele des Rollen- und Berechtigungskonzepts sind:

* Klarheit und Einheitlichkeit bei der Vergabe von Rechten
* Übergreifende, verbindliche Definition der Berechtigungsvergabe
* Verringerung des administrativen Aufwands

## Geltungsbereich

Dieses Rollen- und Berechtigungskonzept gilt für alle Mitarbeiterinnen und Mitarbeiter der [Gemeinde/Stadt]. Die Auftragnehmer im IKT-Bereich werden zur Einhaltung der entsprechenden Anforderungen vertraglich verpflichtet.

## Grundlagen

Die Grundlagen der [Gemeinde/Stadt] sind:

* Gesetz über die Information und den Datenschutz (IDG, [LS 170.4](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4))
* Verordnung über die Information und den Datenschutz (IDV, [LS 170.41](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.41))
* Verordnung über die Informationsverwaltung und -sicherheit (IVSV, [LS 170.8](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.8))
* Stellenbeschreibung der Mitarbeitenden
* Leitlinie zur Informationssicherheit [Gemeinde/Stadt]
* Allgemeine Richtlinie für Informationssicherheit und Datenschutz [Gemeinde/Stadt]
* Weisung zur Informationssicherheit und zum Datenschutz [Gemeinde/Stadt]
* Technische Richtlinie für den Betrieb von Informationssystemen [Gemeinde/Stadt]
* [Entsprechende weitere gesetzliche Grundlagen aufführen]

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen zu beachten.

# Konzeptionelle Vorgaben

## Zugriffskontrolle

Alle eingesetzten IKT-Systeme (Zentralsysteme, Endbenutzersysteme wie PC, Terminalserverclients usw.) sind durch Zugriffskontrolle vor unerlaubter Nutzung zu schützen. Jede Benutzerin und jeder Benutzer wird mindestens durch eine eindeutige Identifikation und ein Passwort gegenüber dem System identifiziert und authentifiziert.

## Zugriffsrechte

Der Zugriff auf Systeme und Anwendungen erfolgt nur nach vordefinierten Rollen und Berechtigungen. Die Berechtigungen werden nach dem Need-to-know-Prinzip vergeben: jede Mitarbeiterin oder jeder Mitarbeiter erhält nur die Rechte, die für ihre/seine Funktion und Tätigkeit erforderlich sind.

## Prozesse

Es sind Prozesse definiert, die die Beantragung, die Prüfung, die Vergabe und die Kontrolle von Berechtigungen nachvollziehbar und vollständig regeln (siehe auch Kapitel 5.2 ff).

Die Berechtigungen für den Zugriff auf IKT-Systeme und Anwendungen werden durch die verantwortlichen Personen gemäss Rollen- und Berechtigungsdefinition geprüft und genehmigt. Kontrollen sind mindestens jährlich (für Mitarbeiterinnen und Mitarbeiter) und halbjährlich (für administrative Zugriffsrechte) durchzuführen.

## Support

Für ausgelagerte Supportaufgaben kann die Administratorin/der Administrator der [Firma] auf die Systeme zugreifen. Der Zugriff findet nur unter Beaufsichtigung durch eine Mitarbeiterin/einen Mitarbeiter der [Gemeinde/Stadt] statt.

## Authentifikation der Benutzerinnen und Benutzer

Grundsätzlich werden alle Benutzerinnen und Benutzer für den Netzwerkzugriff und die jeweiligen Applikationen authentifiziert. Andere Benutzerinnen und Benutzer, zum Beispiel technisch bedingte Benutzer-IDs, werden durch die/den Informationssicherheitsverantwortlichen (ISV), gegebenenfalls in Zusammenarbeit mit dem Betreiber vergeben, dokumentiert und überwacht.

# Funktionsrollen

Die Funktionsrollen bilden die verschiedenen dienstlichen Funktionen der Mitarbeiterinnen und Mitarbeiter innerhalb der [Gemeinde/Stadt] ab. Sie bestehen aus allen für die Funktion notwendigen Zugriffen auf Applikationen und Dateiablage.

Die Rollen sollten möglichst homogen gebildet werden, je nach Grösse des Organs können allerdings Mehrfachfunktionen und entsprechend Zuweisung zu mehreren Rollen notwendig sein.

Ziel der Rollen ist es, bei Eintritt oder Wechsel einer Mitarbeiterin oder eines Mitarbeiters die für die Funktion notwendigen Berechtigungen einheitlich, schnell und nachvollziehbar zuweisen zu können.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rollenbezeichnung | Beschreibung | Anwendungen / Zugriffe | Mitglieder der Rollen | Genehmigung durch |
| LEITUNG\_STEUERN | Abteilungsleiter/in Steuern | NEST  ABACUS  Mail (Exchange)  MS Office  Internetzugang  Verzeichnis «Alle»  Verzeichnis «Steuern»  Verzeichnis «Leitung»  Verzeichnis «Home» | Mitarbeiter/in A | Gemeindeschreiber/in / Stadtschreiber/in |
| MA\_STEUERN | Mitarbeiter/in Abteilung Steuern | NEST  Mail (Exchange)  MS Office  Internetzugang  Verzeichnis «Alle»  Verzeichnis «Steuern»  Verzeichnis «Home» | Mitarbeiter/in B  Mitarbeiter/in C | Abteilungsleiter/in Steuern |
| … |  |  |  |  |

Tabelle 1: Rollendefinitionen am Beispiel einer Gemeinde/Stadt

# Berechtigungen

Ziel der Berechtigungsmatrix ist die konkrete Zuweisung von Einzelrechten auf die verschiedenen Rollen. Sie müssen in den Anwendungen umgesetzt werden. So müssen die Rechte nicht einzeln vergeben werden.

Sollte eine Anwendung die Funktion von Rollendefinitionen und -zuweisungen nicht unterstützen, sind die Einzelrechte dennoch definiert und können anhand der Vorgabe in der Anwendung vergeben werden.

Die Zuweisung der Zugriffsrechte im Dateisystem und in den Anwendungen erfolgt über definierte Gruppen, Organisationseinheiten oder Personen.

Rolle MA\_STEUERN (Beispiel)

|  |  |  |  |
| --- | --- | --- | --- |
| Anwendungen/Verzeichnis | Funktionen/Zugriff | Einschränkung | Bemerkung |
| NEST (Steuern) | Ansicht Dossiers  Bearbeiten Dossiers  Drucken Steuerausweis  … | Ohne Freigabe Einschätzung  Kein Zugriff auf Mitarbeiterinnen und Mitarbeiter Gemeindeverwaltung/Stadtverwaltung | -- |
| ABACUS (Kreditoren) | Ansicht Kreditoren  Bearbeiten Kreditoren  Erfassen Zahlungen  Freigabe Zahlungen | Kompetenz bis CHF 5000.00 | -- |
| MS Office 2019 | MS Outlook  MS Word  MS Excel  MS Powerpoint  MS Visio | -- | -- |
| Interzugang | MS Internet Explorer | -- | -- |
| Verzeichnis «Alle» | Lesen/Schreiben/Löschen | -- | -- |
| Verzeichnis «Home» | Lesen/Schreiben/Löschen | -- | Verzeichnis pro Benutzenden |
| Verzeichnis «Steuern» | Lesen/Schreiben/Löschen | -- | -- |
| Verzeichnis «Info» | Lesen |  |  |
| … |  |  |  |

Tabelle 2: Berechtigungsmatrix am Beispiel einer Rolle

Zur besseren Übersicht kann eine Matrix aller Mitarbeiterinnen und Mitarbeiter sowie aller Rollen gebildet werden, woraus die Zuteilung klar ersichtlich wird.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Benutzer | Rolle 1 | Rolle 2 | Rolle 3 | Rolle 4 | Rolle 5 | Rolle 6 | Rolle 7 | Rolle 8 | Rolle 9 | Rolle 10 |
| Mitarbeiter/in A | X |  |  | X |  |  |  |  |  |  |
| Mitarbeiter/in B |  | X |  |  |  |  |  |  |  |  |
| Mitarbeiter/in C |  |  |  |  | X |  |  |  |  |  |
| Mitarbeiter/in D |  |  |  |  |  | X | X |  |  |  |
| Mitarbeiter/in E |  |  |  |  | X |  |  | X |  |  |
| … |  |  |  |  |  |  |  |  |  |  |

Tabelle 3: Beispiel einer Zuteilungsmatrix

# Verantwortlichkeiten und Prozesse

Nachfolgend sind die Verantwortlichkeiten und Einzelprozesse im Zusammenhang mit Rollen und Berechtigungen beschrieben.

Hinweis: Wenn mehrere Funktionen durch dieselbe Person wahrgenommen werden, sind mögliche Interessenkonflikte durch unterschiedliche Rollen zu verhindern (Funktionstrennung/Segregation of Duties).

## Verantwortlichkeiten

Personalverantwortliche

* Melden personeller Mutationen an die Daten- und Anwendungsverantwortliche/den Daten- und Anwendungsverantwortlichen bzw. die/den ISV

Vorgesetzte

* Prüfen und Freigeben von Berechtigungsanträgen
* Regelmässiges Überprüfen der bestehenden Berechtigungen in Zusammenarbeit mit der/dem ISV sowie den Daten- und Anwendungsverantwortlichen

Daten- und Anwendungsverantwortliche

* Definieren und Anpassen der Funktionsrollen
* Zuweisen von Personen zu Rollen
* Definieren und Anpassen der Berechtigungsmatrix (Zugriffsberechtigungen pro Rolle)
* Erstellen von Ausnahmebewilligungen (Zugriffsberechtigungen für Mitarbeiterinnen und Mitarbeiter ausserhalb der Rollen, Gewährung von Einzelberechtigungen)
* Prüfen und bestätigen von Berechtigungsanträgen
* Regelmässiges Überprüfen der bestehenden Rollen und Zuteilungen auf Richtigkeit und Zweckmässigkeit (falls nötig Einleiten von Korrekturmassnahmen) in Zusammenarbeit mit der/dem ISV

Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher

* Generieren eines Initialpassworts beim erstmaligen Einrichten von Zugriffen zur einmaligen Nutzung (resp. Beauftragen des IKT-Betreibers)
* Eröffnen von Benutzer- und Gruppennamen gemäss einer festgelegten Namenskonvention
* Zurücksetzen des Passworts (wo möglich sind Self-Service-Funktionen zu bevorzugen)
* Bearbeiten aller Fragen und Probleme rund um Zugriffe und Passwörter
* Zurverfügungstellen von Berechtigungslisten für die regelmässige Überprüfung der Zugriffe auf Richtigkeit und Zweckmässigkeit
* Überwachen der Überprüfungen
* Korrektes und vollständiges Ablegen der Aufträge zur Sicherstellung der Nachvollziehbarkeit

Administratorin/Administrator Netzwerk und Systeme

* Vergeben von Berechtigungen und Anmeldedefinitionen (Benutzer-ID und Passwort) auf Netzwerkkomponenten (Router, Switches, Firewall), Server- und Client-Systemen, E-Mail-Systemen und weiteren.

Administratorin/Administrator Anwendungen und Datenbanken

* Vergeben von applikationsbezogenen Berechtigungen (Zugriffe auf Daten, Prozesse wie Masken und Reports sowie Drucker usw.) und Anmeldedefinitionen (Benutzer-ID und Passwort).

## Prozess Einrichten / Ändern von Zugriffsberechtigungen

Prozess: Personalverantwortliche/r →

Vorgesetzte/r →

Mitarbeiter/in →

Daten- und Anwendungsverantwortliche/r →

ISV

Medium: Auftrag per [Ticket/Mail], Rückmeldung per [Ticket/Mail]

Authentifizierung: Persönlich bekannt, ansonsten Ausweis

Initialpasswort: Durch Daten- und Anwendungsverantwortliche/n definiert

## Löschen von Zugriffsberechtigungen

Prozess: Personalverantwortliche/r →

ISV →

Bei Bedarf externer Dienstleister

Medium: Auftrag per [Ticket/Mail], Rückmeldung per [Ticket/Mail]

## Einrichten / Zurücksetzen des Passworts

Die Aufträge sind durch die verantwortliche Stelle auf Authentizität und Richtigkeit zu überprüfen.

Prozess: Mitarbeiter/in →

ISV →

Medium: Auftrag per Mail, Rückmeldung per Telefon/E-Mail

Authentifizierung: Persönlich bekannt, ansonsten Ausweis

# Genehmigung und Inkrafttreten

Beschlossen durch [die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber] am [Datum]

[Ort und Datum] [Name]

[Gemeinde/Stadt] [Gemeindeschreiberin/Gemeindeschreiber / Stadtschreiberin/Stadtschreiber]

V 1.3 / Oktober 2024