GEMEINDE
Niederglatt

Rollen- und Berechtigungskonzept zur Informationssicherheit

der Politischen Gemeinde Niederglatt

(Rollen- und Berechtigungskonzept)

Festgesetzt mit GRB vom:	02.09.2019
In Kraft getreten am:	02.09.2019

Gemeinde Niederglatt | Grafschaftstrasse 55 | 8172 Niederglatt | Tel. 044 852 20 40 | Fax 044 850 05 08 | www.niederglatt-zh.ch

1. Gegenstand und Zweck

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

Ziele des Rollen- und Berechtigungskonzepts sind:

- Klarheit bei der Vergabe von Rechten
- Übergreifende, verbindliche Definition der Berechtigungsvergabe
- Verringerung des administrativen Aufwandes

Wichtige Eckpunkte sowie den Berechtigungen zugrundeliegende Annahmen werden beschrieben.

2. Geltungsbereich

Dieses Rollen- und Berechtigungskonzept gilt für alle Mitarbeitenden der Gemeinde Niederglatt. Die Auftragnehmenden im IT-Bereich werden vertraglich zur Einhaltung der entsprechenden Anforderungen 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 respektive beim Gemeindeschreiber. Sie respektive er delegiert die Aufgaben und Kompetenzen an die Daten- und Anwendungsverantwortlichen und/oder an die IT-Verantwortliche.

3.2 Grundlagen

Folgende Grundlagen und Dokumente enthalten Aspekte der Verantwortlichkeit:

- Gemeindeordnung vom 29.11.2009
- Geschäftsordnung des Gemeinderats vom 21.03.2011
- Leitlinie zur Informationssicherheit vom 02.09.2019
- Stellenbeschreibung der Mitarbeitenden

3.3 Risikobeurteilung und Sicherheitsstufe

Die Zuordnung der Informationen erfolgt aufgrund der Risikoanalyse in die Sicherheitsstufe S2 nach ISV (Informatiksicherheitsverordnung, LS 170.8). Alle Systeme, Anwendungen und Informationen der Gemeinde werden im vorliegenden Konzept berücksichtigt.

3.4 Prozesse

Die **Berechtigungen** für den Zugriff auf IT-Systeme und -Anwendungen werden durch die Daten- und Anwendungsverantwortlichen oder den IT-Verantwortlichen sorgfältig eingerichtet. Sie sorgen für deren permanente Nachführung respektive Aktualität.

Zugriffe auf Informationen ist nur bewilligten Zugriffsgruppen und damit denjenigen Mitarbeitenden, deren Berechtigung schriftlich vergeben wurde, zu gewähren. Dies dient dem Schutz der Integrität (Richtigkeit, Vollständigkeit) der Informationen.

Treten Fehler in den Anwendungen auf, die zur Verletzung der Integrität führen oder die Verfügbarkeit der gespeicherten Informationen gefährden können, sind diese abzuklären und entsprechende Massnahmen einzuleiten.

3.5 Zugriffskontrolle

Alle eingesetzten IT-Systeme (Zentralsysteme, Endbenutzersysteme wie PC, Terminal Server Clients usw.) sind mittels Zugriffskontrolle vor unerlaubter Nutzung zu schützen. Alle Anwendenden werden mindestens mittels einer Identifikation und durch ein Passwort gegenüber dem System identifiziert und authentifiziert.

4. Funktionen

4.1 Funktionen im IT-Bereich

Die nachfolgenden, verschiedenen Funktionen werden durch den IT-Verantwortlichen wahrgenommen. Davon ausgenommen ist der Bereich der Revision und bei einer Auslagerung die Administratorenrolle, die vom extern beauftragten IT-Dienstleister (Abraxas/VRSG) wahrgenommen wird.

4.1.1 Informationssicherheitsverantwortlicher

Der Informationssicherheitsverantwortliche überwacht alle getroffenen Massnahmen der externen Auftragnehmenden und prüft regelmässig die Einhaltung der Sicherheitszielsetzungen. Er setzt die Informatiksicherheitsverordnung um und regelt den Ablauf der regelmässigen Prüfung gemäss § 18 ISV. Er plant die Sensibilisierung und Schulung für die Informationssicherheit und führt diese zusammen mit den Daten- und Anwendungsverantwortlichen durch. Er ist Anlauf- und Meldestelle für Probleme und Beobachtungen im Bereich Informationssicherheit. Er rapportiert dem Gemeindeschreiber und den Daten- und Anwendungsverantwortlichen.

4.1.2 IT-Verantwortliche / IT-Verantwortlicher

Die oder der IT-Verantwortliche betreut die IT-Infrastruktur der Gemeinde.

4.1.3 Administrator – Netzwerk und Systeme (wahrgenommen durch Abraxas/VRSG)

Die Administratoren betreiben und unterhalten die Netzwerkkomponenten (Router, Switches, Firewall), die Server- und Client-Basissysteme (Betriebssystem und betriebssystemnahe Software), E-Mail-Systeme und Büroautomationsprogramme.

4.1.4 Administratorin / Administrator – Anwendungen und Datenbanken (wahrgenommen durch Abraxas/VRSG)

Die Administratoren vergeben alle applikationsbezogenen Rechte (Zugriffe auf Daten, Prozesse wie Masken und Reports sowie Drucker usw.) und Anmeldedefinitionen (Benutzenden-ID und Passwort). Zusätzlich werden durch sie die Datenbanksysteme in technischer Hinsicht betrieben und unterhalten.

4.1.5 Revision

Unabhängige Stellen prüfen gemäss § 18 ISV die rechtlichen, organisatorischen und technischen Massnahmen im IT-Bereich auf der Basis der ISV und der Leitlinie zur Informationssicherheit respektive dem IT-Sicherheitskonzept.

4.2 Zuweisung der Funktion zu Stelle bzw. Person

Gemäss separatem Anhang in den „Leitlinie Informationssicherheit“ vom 02.09.2019. Mehrere Funktionen können aufgrund der Grösse der Gemeinde durch dieselben Mitarbeitenden wahrgenommen werden.

5. Zugriffsdefinitionen

Die Gemeinde Niederglatt verfügt über eine Dokumentation der Dateien, Prozesse und Systeme, der diesen Objekten zugewiesenen Gruppen und deren Berechtigungen (lesen, bearbeiten, voller Zugriff). Die Dokumentation wird aufgrund der auf dem System und in den Anwendungen vorhandenen Definitionen erstellt. Die Administratoren (IT-Verantwortliche und externer IT-Dienstleister VRSG) und die Personen mit Stellvertretung haben Zugriff auf alle Informationen inklusive Systemdaten und Prozesse, die ausschliesslich dem Betrieb der IT-Umgebung dienen.

6. Zugriffsrechte im Dateisystem und in Anwendungen

Die Zuweisung der Zugriffsrechte im Dateisystem und in den Anwendungen erfolgt über die Gruppen an die jeweiligen Mitarbeitenden bzw. Stellen. Die Zugriffsrechte sind auf separaten Übersichtslisten des extern beauftragten IT-Dienstleisters (Abraxas/VRSG) festgehalten und werden durch den IT-Verantwortlichen der Gemeinde Niederglatt regelmässig auf ihre Richtigkeit hin überprüft.

7. Einrichten / Ändern / Löschen der Zugriffsrechte und des Passworts

Der Gemeindeschreiber meldet dem IT-Verantwortlichen die Anforderungen. Beim erstmaligen Einrichten der Berechtigungen wird ein Initialpasswort durch den IT-Verantwortlichen definiert. Für die Benützer- und Gruppennamen wird eine Namenskonvention eingehalten. Der IT-Verantwortliche hat folgende Aufgaben:

- 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
- Beantwortung aller Fragen und Probleme rund um Zugriffe und Passwörter

8. Weitere Massnahmen

8.1 Authentifizierung der Benutzenden

Grundsätzlich werden alle Benutzenden auf dem Netzwerk und in den Applikationen authentisiert. Andere Benutzende (wie zum Beispiel technisch bedingte IDs) werden durch den extern beauftragten IT-Dienstleister (Abraxas/VRSG) vergeben, dokumentiert und permanent überwacht.

8.2 Dokumentation für Applikationen

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

8.3 Lokale Netze, Fremdnetze und Internet

Die Firma Abraxas/VRSG, in der Funktion Administrator Netzwerke, betreibt und unterhält die Netzwerkkomponenten und die Abtrennung des internen Netzwerks von Fremdnetzen (Firewall). Sie informiert und dokumentiert betreffend die 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).

8.4 Lokale Administration auf dem Client, Fernzugriff

Die lokale Administration auf dem Client wird durch den IT-Verantwortlichen der Gemeinde Niederglatt oder durch Mitarbeitende des extern beauftragten IT-Dienstleisters Abraxas/VRSG durchgeführt. Die technische Administration wird durch Mitarbeitende des extern beauftragten IT-Dienstleisters Abraxas/VRSG sowie durch den IT-Verantwortlichen der Gemeinde Niederglatt durchgeführt. Die Abraxas/VRSG kann von extern – unter Einbezug eines Benutzenden – auf die Systeme zugreifen. Der Benutzende muss dies vorgängig bestätigen. Im Bereich der Hauptapplikationen (Abraxas/VRSG Fachapplikationen) wird die technische Administration durch die Firma Abraxas/VRSG durchgeführt. Bei den Programmen, welche nicht als Abraxas/VRSG Fachprogramme deklariert sind, werden die Berechtigungen durch den IT-Verantwortlichen der Gemeinde Niederglatt oder einem Drittlieferanten eingerichtet.

8.5 Protokollierung

8.5.1 Zugriff auf besondere Personendaten

Die Daten- und Anwendungsverantwortlichen und/oder der IT-Verantwortliche treffen bei besonderen Vorfällen (Zugriffsverletzungen, Integritätsproblemen mit Daten usw.) in Absprache mit dem Gemeindeschreiber die notwendigen Massnahmen zur Bewahrung der Vertraulichkeit und der Integrität.

8.5.2 Identifizierung und Authentifizierung

Zugriffverletzungen an den Netzwerkgrenzen und an den Systemen werden aufgezeichnet und in Zusammenarbeit mit den Auftragnehmenden bei Bedarf ausgewertet.

9. Genehmigung und Inkraftsetzung

Das Rollen- und Berechtigungskonzept der Gemeinde Niederglatt wurde durch den Gemeindeschreiber, in Zusammenarbeit mit den Verwaltungsabteilungen, erarbeitet und durch den Gemeinderat Niederglatt am 02.09.2019 genehmigt und per sofort in Kraft gesetzt.

Niederglatt, 02. September 2019

GEMEINDERAT NIEDERGLATT

Stefan Schmid	Bruno Schlatter
Gemeindepräsident	Gemeindeschreiber

Schutzbedarfsfeststellung Fachanwendungen

Gemeinde Niederglatt

N	Zweck	Anwendungsname	Vertraulichke	Integrität	Verfügbarkeit	Verantwortung Intern	Verantwortung Extern	Daten-standort
1	Protokollverwaltung	AIB	**H**	**H**	N	Gemeindeschreiber-Stv.	Axians Ruf AG	Extern
2	Scanning Steuererklärungen	ARTS	**H**	N	N	AL Steuern	UPTIME Services AG	Extern
3	Internetaufttritt	CMS iWeb	N	N	N	Gemeindeschreiber-Stv.	Innovative Web AG	Extern
4	Raumreservation	RBS iWeb	N	N	N	Gemeindeschreiber-Stv.	Innovative Web AG	Extern
5	Hundekontrolle	Amicus	N	N	N	SB EWK und Sicherheit	Abraxas AG	Extern
6	Arbeitszeiterfassung	Kelio	N	N	N	Gemeindeschreiber	BMZ - Borsari + Meier AG	Extern
7	Sozialhilfe	Klib	**H**	N	N	AL Soziales	Diartis AG	Extern
8	Feuerwehr	Lodur	N	**H**	**H**	Feuerwehr	Kanton Zürich	Extern
9	Parkierungskonzept	OM Police	**H**	N	N	AL EWK und Sicherheit	OM Computer Support AG	Extern
10	Layout Mitteilungsblatt	indesign	N	N	N	SB EWK und Sicherheit	Adobe	Extern
11	Grundstückgewinnsteuer	Spider Soft	**H**	N	N	AL Finanzen	Spider Soft AG	Extern
12	Finanzbuchhaltung	Abraxas FIS	**H**	N	N	AL Finanzen	Abraxas AG	Extern
13	Anlagebuchhaltung	Abraxas FIS	N	N	N	AL Finanzen	Abraxas AG	Extern
14	Einwohnerkontrolle	Loganto	N	**H**	N	AL EWK und Sicherheit	Abraxas AG	Extern
15	Lohnverwaltung	Abraxas HR Personalm	**H**	N	N	AL Finanzen	Abraxas AG	Extern
16	Steuern	Abraxas ZüriPrimo	**H**	N	N	AL Steuern	Abraxas AG	Extern
17	Wahlen	Wabsti	**H**	**H**	**H**	Gemeindeschreiber	Abraxas AG	Extern
18	Werk Gebühren Fakturierung	Abraxas Gebühren	**H**	N	N	AL Finanzen	Abraxas AG	Extern
19	Organisation Gemeinde Niederglatt	OrgNGL	N	N	N	Gemeindeschreiber-Stv.	Sevitec Imformatik AG	Extern
20	Sozialversicherungen	SVA	**H**	N	N	AL EWK und Sicherheit	SVA Zürich	Extern
21	Kassensystem	TCPos EFT/POS	N	N	N	AL Finanzen	Six Multipay	Extern
22	AHV-Zusatzleistungen	Zuscal	**H**	N	N	AL Soziales	Herbert Schaub AG	Extern

02. September 2019

Schutzbedarfskategorien	
Normal	
Verstoss gegen Gesetze / Vorschriften / Verträge	Verstösse gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Es handelt sich um personenbezogene Daten, durch deren Bearbeitung Betroffene in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigt werden können.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung erscheint nicht möglich.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist grösser als 24 Stunden.
Negative Innen- oder Aussenwirkung	Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der finanzielle Schaden bleibt für die Institution tolerabel.
Hoch	
Verstoss gegen Gesetze / Vorschriften / Verträge	Verstösse gegen Vorschriften und Gesetze mit erheblichen Konsequenzen Vertragsverletzungen mit hohen Konventionalstrafen
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Es handelt sich um personenbezogene Daten, bei deren Bearbeitung Betroffene in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden können.
Beeinträchtigung der persönlichen Unversehrtheit	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Die maximal tolerierbare Ausfallzeit liegt zwischen 1 und 24 Stunden.
Negative Innen- oder Aussenwirkung	Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
Finanzielle Auswirkungen	Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.
Sehr hoch	
Verstoss gegen Gesetze / Vorschriften / Verträge	Fundamentaler Verstoss gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden existenzbedrohend sind
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Es handelt sich um personenbezogene Daten, bei deren Bearbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit von Betroffenen gegeben ist.
Beeinträchtigung der persönlichen Unversehrtheit	Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. Gefahr für Leib und Leben
Beeinträchtigung der Aufgabenerfüllung	Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
Negative Innen- oder Aussenwirkung	Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
Finanzielle Auswirkungen	Der finanzielle Schaden ist für die Institution existenzbedrohend.