Pfungen
Leben an der Töss

Rollen- und Berechtigungskonzept

vom 25. November 2019

Änderungsverlauf

Version	Datum	Text	Instanz
2019	25.11.2019	Rollen- und Berechtigungskonzept	Gemeinderat (GRB Nr. 206)

Inhaltsverzeichnis

1. Allgemeine Bestimmungen

Art. 1

Gegenstand und Zweck

Das Rollen- und Berechtigungskonzept dient dem Schutz der Vertraulichkeit und der Integrität. Dieses Dokument ist die Grundlage 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

Art. 2

Geltungsbereich

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

2. Konzeptionelle Vorgaben

Art. 3

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.

Art. 4

Grundlagen

Folgende Grundlagen und Dokumente enthalten Aspekte der Verantwortlichkeit:

- Gemeindeordnung vom 24.09.2017
- Geschäftsordnung des Gemeinderates vom 15.03.2010
- Leitlinie zur Informationssicherheit vom 03.09.2019
- Stellenbeschreibung der Mitarbeitenden

Art. 5

Risikobeurteilung und Sicherheitsstufe

Die Zuordnung der Informationen erfolgt aufgrund der Risikoanalyse in die Sicherheitsstufe S 1 (S1) nach Informatiksicherheitsverordnung (ISV, LS 170.8). Alle Systeme, Anwendungen und Informationen der Gemeinde Pfungen werden im diesem Konzept berücksichtigt.

Art. 6

Prozesse

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

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

Art. 7

Zugriffskontrolle

[1] 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.

[2]. Der Auftragnehmende in der Funktion Administrator Netzwerke 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).

Art. 8

Support

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

3. Funktionen

Art. 9

Funktionen innerhalb der Gemeinde

Gemäss Organigramm im Anhang

Mehrere Funktionen könne aufgrund der Grösse der Gemeinde durch dieselben Mitarbeitenden wahrgenommen werden.

Art. 10

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 Ruf Informatik AG wahrgenommen wird.

- IT-Verantwortliche / IT-Verantwortlicher

Die oder der IT-Verantwortliche betreut die IT-Infrastruktur der Gemeinde Pfungen, überwacht alle getroffenen IT-Massnahmen der externen Auftragnehmenden und prüft regelmässig die Einhaltung der Sicherheitszielsetzungen. Sie oder er setzt die Informatiksicherheitsverordnung um, regelt den Ablauf der regelmässigen Prüfung gemäss § 18 ISV, 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 den Gemeindeschreiber sowie den Daten- und Anwendungsverantwortlichen.

- 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.

- IT-Verantwortliche / IT-Verantwortlicher – Anwendungen und Datenbanken

Der oder die IT-Verantwortliche vergibt zusammen mit der OBT AG alle applikationsbezogenen Rechte (Zugriffe auf Daten, Prozesse wie Masken und Reports sowie Drucker usw.) und Anmeldedefinitionen (Benutzer-ID und Passwort).
Zusätzlich werden durch die OBT AG die Datenbanksysteme in technischer Hinsicht betrieben und unterhalten.

- Revision

Die periodischen Kontrollen nach § 18 ISV erfolgen durch die Abteilung Recht und IT-Sicherheit des kantonalen Datenschutzbeauftragen.

Art. 11

Zugriffsrechte

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

Tabelle 1 siehe Anhang 2

Tabelle 2 siehe Anhang 3

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

Art. 12

Berechtigungen

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.

Art. 13

Verantwortlichkeiten

1. 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

2. 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.

3. 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).

Art. 14

Prozesse

1. Standard

Prozess:	Daten- und Anwendungsverantwortliche→IT-Verantwortliche/-r
Medium:	Auftrag per Ticket, Rückmeldung per Mail
Authentifizierung:	Persönlich bekannt, ansonsten Ausweis
Initialpasswort:	Durch Daten- und Anwendungsverantwortliche definiert

2. Windows Active Directory (Dateiserver)

Prozess:	Personal→Daten- und Anwendungsverantwortliche→IT-Verantwortliche/r
Medium:	Auftrag per Ticket, Rückmeldung per Mail
Authentifizierung:	Persönlich bekannt, ansonsten Ausweis
Initialpasswort:	Durch die IT-Verantwortliche / IT-Verantwortlicher definiert

Art. 15

Meldestelle

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

5. Weitere Massnahmen

Art. 16

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 die verantwortliche Person vergeben, dokumentiert und überwacht.

Art. 17

Dokumentation für Applikationen

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

Art. 18

Lokale Netze, Fremdnetze und Internet

Die zuständige Person in der Funktion Administrator Netzwerke unterhält und betreibt 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).

Art. 19

Lokale Administration auf dem Client, Fernzugriff

Die lokale Administration auf dem Client wird durch die IT-Verantwortlichen durchgeführt. Die technische Administration wird durch die zuständige Person 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 die zuständige Stelle durchgeführt.

6. Inkraftsetzung

Art. 20

Akten der Ressortleiter

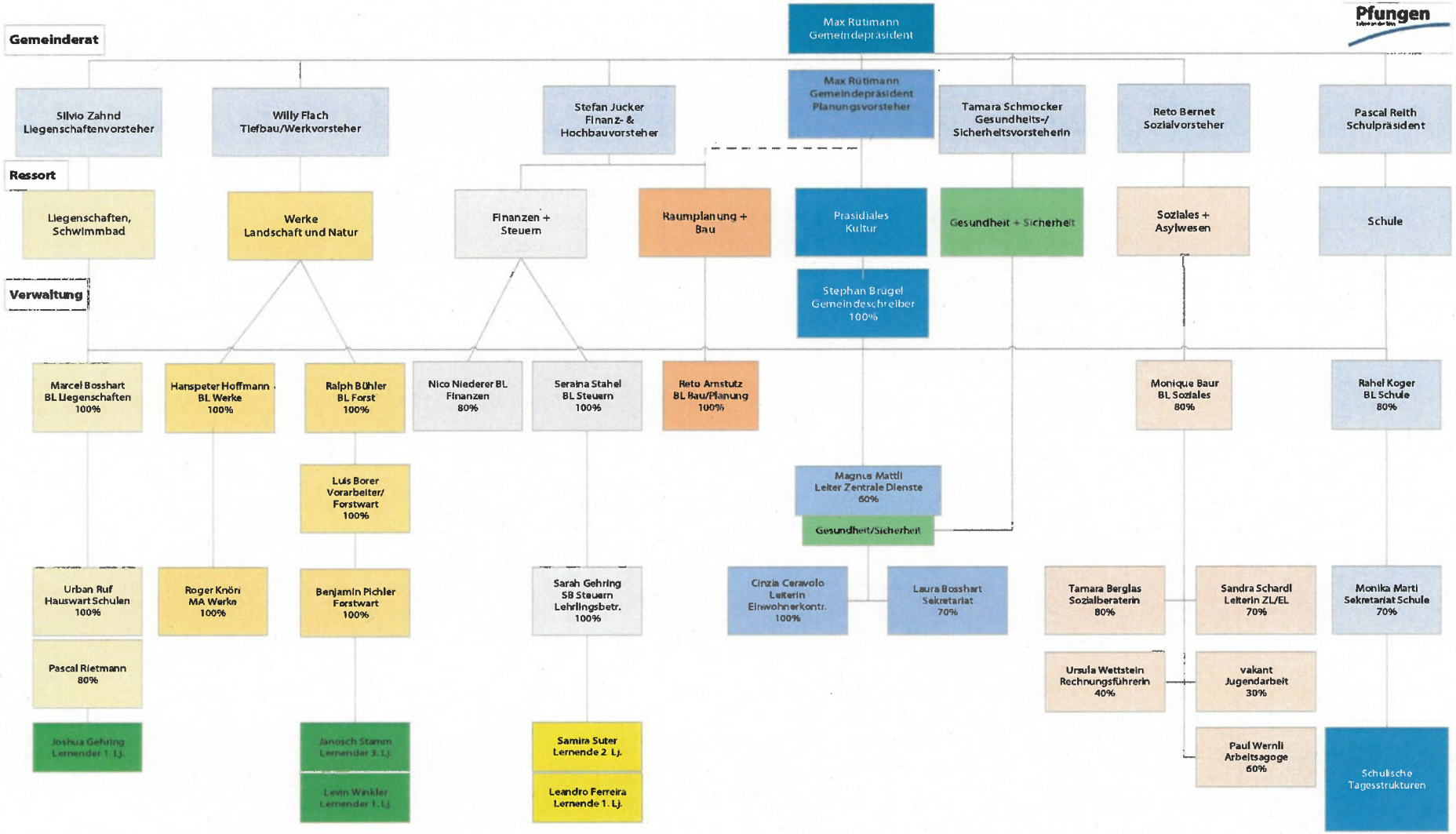
Der Gemeinderat setzt das vorliegende Rollen- und Berechtigungskonzept per 01. Dezember 2019 in Kraft.

Pfungen, 25. November 2019
Gemeinderat Pfungen

Max Rütimann
Gemeindepräsident

Stephan Brügel
Gemeindeschreiber

Anhang 1



V. 01.12.2019

Anhang 2

Tabelle 1 – Zugriffsmatrix am Beispiel einer Gemeinde

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	...	...	...
...	...	...	...

Anhang 3

Tabelle 2 – Zugriffsmatrix am Beispiel einer Gemeinde

Rollenbezeichnung	Beschreibung	Funktionen / Zugriff	Mitglieder der Rolle	Genehmigung durch
Baupro	…	Administrator/-in Geschäfte erfassen …	… … …	…
GEVER, BrainConnect	…	Administrator/-in Geschäfte erfassen …	… … …	…
W+W (Finanzbuchhaltung)	…	Administrator/-in Rechnungen ausstellen Rechnungen genehmigen	… … …	…
W+W (Lohn)	…	Administrator/-in Lohn ändern …	… … …	…
W+W (Einwohnerkontrolle)	…	Administrator/-in Einwohner mutieren …	… … …	…
W+W (Steuern)	…	Administrator/-in Steuerausweis drucken	… … …	…
Scolaris	…	…	… … …	…
Internet (CMSi-Webh)	…	…	… …	…
Extranet (CMSi-Webh)	…	…	… …	…
Exchange	…	…	…	…
…	…	…	…	…