PRIMARSCHULE TRUTTIKON

IT Rollen- und Berechtigungskonzept

1 Allgemeine Bestimmungen

1.1 Gegenstand und Zweck

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

Ziele des Rollen- und Berechtigungskonzepts sind:

- Klarheit und Einheitlichkeit bei der Vergabe von Rechten
- Übergreifende, verbindliche Definition der Berechtigungsvergabe

1.2 Geltungsbereich

Dieses Rollen- und Berechtigungskonzept gilt für alle Mitarbeiterinnen und Mitarbeiter der PS Truttikon.

1.3 Grundlagen

Folgende Grundlagen und Dokumente enthalten Aspekte der Verantwortlichkeit:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Verordnung über die Informationsverwaltung und -sicherheit (IVSV, LS 170.8)
- Geschäftsordnung der Schulpflege vom
- Stellenbeschreibung der Mitarbeitenden
- Allgemeine Richtlinie für Informationssicherheit und Datenschutz PS Truttikon
- Weisung zur Informationssicherheit und zum Datenschutz PS Truttikon

2 Konzeptionelle Vorgaben

2.1 Zugriffskontrolle

Alle eingesetzten IT-Systeme 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.

2.2 Zugriffsrechte

Der Zugriff auf Systeme und Anwendungen erfolgt nur nach vordefinierten Rollen und Berechtigungen.Jede Mitarbeiterin oder jeder Mitarbeiter erhält die Rechte, die für ihre/seine Funktion und Tätigkeit erforderlich sind.

2.3 Support

Für ausgelagerte Supportaufgaben kann der Administrator der Supportfirma auf die Systeme zugreifen. Der Zugriff findet nur unter Beaufsichtigung durch eine Mitarbeiterin/einen Mitarbeiter der PS Truttikon statt.

3 Funktionsrollen

Die Funktionsrollen bilden die verschiedenen dienstlichen Funktionen der Mitarbeiterinnen und Mitarbeiter innerhalb der PS Truttikon ab. Sie bestehen aus allen für die Funktion notwendigen Zugriffen auf Applikationen und Dateiablage.

Text einfügen…

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	Berechtigung
SCHULLEITUNG	Schulleiter/in	PULS-ZH	Zugriff
		Lehrer Office	Admin
		Mail	Zugriff
		MS Office	Zugriff
		Internetzugang	Zugriff
		Verzeichnis «Alle und Schüler»	Bearbeiten
		Verzeichnis «Lehrer»	Bearbeiten
		Verzeichnis «Schulleitung»	Bearbeiten
		Verzeichnis «Verwaltung»	Bearbeiten
LEHRPERSONAL	Lehrperson	Lehrer Office	Zugriff
		Mail	Zugriff
		MS Office	Zugriff
		Internetzugang	Zugriff
		Verzeichnis «Alle»	Bearbeiten
		Verzeichnis «Home»	Bearbeiten
		Verzeichnis «Lehrer»	Bearbeiten
		Verzeichnis «Schüler»	Bearbeiten
Verwaltung	Sekretariat	Lehrer Office	Admin
		Mail	Zugriff
		MS Office	Zugriff
		Internetzugang	Zugriff
		Verzeichnis «Alle»	Bearbeiten
		Verzeichnis «Home»	Bearbeiten
		Verzeichnis «Verwaltung»	Bearbeiten

4 Verantwortlichkeiten und Prozesse

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

Personalverantwortliche

– Melden personeller Mutationen an die Daten- und Anwendungsverantwortliche

Schulleitung/DSB

– Prüfen und Freigeben von Berechtigungsanträgen

IT/Datenschutzbeauftragter

– Definieren und Anpassen der Funktionsrollen
– Zuweisen und überprüfen 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)
– 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)