Vorlage Rollen- und Berechtigungskonzept [SCHULE]



Inhalt

[1. Allgemeine Bestimmungen 3](#_Toc192858175)

[1.1. Gegenstand und Zweck 3](#_Toc192858176)

[1.2. Geltungsbereich 3](#_Toc192858177)

[1.3. Grundlagen 3](#_Toc192858178)

[2. Konzeptionelle Vorgaben 3](#_Toc192858179)

[2.1 Prozesse 3](#_Toc192858180)

[2.2 Zugriffskontrolle 3](#_Toc192858181)

[2.3 Zugriffsrechte 4](#_Toc192858182)

[2.4 Support 4](#_Toc192858183)

[2.5 Authentifikation der Benutzerinnen und Benutzer 4](#_Toc192858184)

[3. Funktionsrollen 4](#_Toc192858185)

[4. Berechtigungen 5](#_Toc192858186)

[5. Verantwortlichkeiten und Prozesse 5](#_Toc192858187)

[5.1 Verantwortlichkeiten 6](#_Toc192858188)

[5.2 Prozess Einrichten / Ändern von Zugriffsberechtigungen 6](#_Toc192858189)

[5.3 Löschen von Zugriffsberechtigungen 7](#_Toc192858190)

[5.4 Einrichten / Zurücksetzen des Passworts 7](#_Toc192858191)

[Anhang I– Dynamisch anpassbar (Rolle-Mitarbeiter) 8](#_Toc192858192)

# Allgemeine Bestimmungen

## Gegenstand und Zweck

Das Rollen- und Berechtigungskonzept dient dem Schutz der Vertraulichkeit und der Integrität. Dieses Dokument ist die Grundlage für die [SCHULE] 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 Mitarbeitenden sowie Lernenden der [SCHULE]. Die Auftragnehmenden im IKT-Bereich werden zur Einhaltung der entsprechenden Anforderungen vertraglich verpflichtet.

## Grundlagen

Folgende Grundlagen und Dokumente enthalten Aspekte der Verantwortlichkeit:

* Regelungen und Weisungen der Schule
* Allgemeine Richtlinie zur Informationssicherheit und Datenschutz vom [DATUM]
* Stellenbeschreibung der Mitarbeitenden

# Konzeptionelle Vorgaben

## 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.

## Zugriffskontrolle

Alle eingesetzten IKT-Systeme (Zentralsysteme, Endbenutzersysteme wie PC usw.) sind durch Zugriffskontrolle vor unerlaubter Nutzung zu schützen. Jeder Anwendende wird mindestens durch eine Identifikation und ein Passwort gegenüber dem System identifiziert und authentifiziert. Für kritische Systeme ist eine Multi Faktor Authentifizierung notwendig.

## 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.

## Support

Für ausgelagerte Supportaufgaben kann die Administratorin/der Administrator der [Firma] auf die Systeme zugreifen. Der Zugriff findet wenn möglich unter Beaufsichtigung durch eine Mitarbeiterin/einen Mitarbeiter der [Schule] statt. Die [Firma] unterzeichnet eine Geheimhaltungserklärung. In der Geheimhaltungserklärung verpflichtet sich die [Firma] nur Aufgaben im Bereich des Auftrags zu erledigen und keine Informationen preis zu geben.

## 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 [Schule] 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.

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| System | Student-SekII | Teacher-SekII | Secretariat-SekII | Personal-SekII | Management-SekII | Committee-SekII | Users-SekII |
| System A | r |  |  | r/d/w |  |  |  |
| System B |  | r/w |  |  |  |  |  |
| System C |  |  |  |  | r/d/w |  |  |
| System D |  |  |  |  |  | r/d/w | r |
| System E |  |  | r/d/w |  | r |  |  |
| … |  |  |  |  |  |  |  |

Tabelle 1: Beispiel einer Zuteilungsmatrix

r = read (lesen)

d = delete (löschen)

w = write (schreiben)

# 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 Rollen. Die Zuweisung der einzelnen Rollen zu den Mitarbeitenden ist im Anhang I – Dynamisch anpassbar (Rolle-Mitarbeiter) festgehalten.

# 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

Anwendungs- und Datenverantwortliche

* Zuweisen von Personen zu Rollen
* Beantragen von Ausnahmebewilligungen (Zugriffsberechtigungen für Mitarbeiterinnen und Mitarbeiter ausserhalb der Rollen, Gewährung von Einzelberechtigungen)

Informationssicherheitsverantwortliche/Informationssicherheitsverantwortlicher

* Generieren eines Initialpassworts beim erstmaligen Einrichten von Zugriffen zur einmaligen Nutzung (resp. Beauftragen des IKT-Betreibers)
* Zurücksetzen des Passworts (wo möglich sind Self-Service-Funktionen zu bevorzugen)
* Bearbeiten aller Fragen und Probleme rund um Zugriffe und Passwörter
* Korrektes und vollständiges Ablegen der Aufträge zur Sicherstellung der Nachvollziehbarkeit

**Nachfolgende Verantwortlichkeiten sind in der IKT-Grundversorgung nicht bei der Schule angesiedelt.**

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 [Ticket/Mail], Rückmeldung per Telefon/E-Mail

Authentifizierung: Persönlich bekannt, ansonsten Ausweis

V1.0 / März 2025

# Anhang I– Dynamisch anpassbar (Rolle-Mitarbeiter)

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Mitarbeiter | Student-SekII | Teacher-SekII | Secretariat-SekII | Personal-SekII | Management-SekII | Committee-SekII | Users-SekII |
| Mitarbeiter/in A | X |  |  | X |  |  |  |
| Mitarbeiter/in B |  | X |  |  |  |  |  |
| Mitarbeiter/in C |  |  |  |  | X |  |  |
| Mitarbeiter/in D |  |  |  |  |  | X | X |
| Mitarbeiter/in E |  |  |  |  | X |  |  |
| … |  |  |  |  |  |  |  |

Tabelle 2: Rollendefinitionen am Beispiel einer Mittel- oder Berufsfachschule