

Zugriffs- und Berechtigungsmanagement (On- und Offboarding)

Berechtigungen werden für unterschiedliche Systeme verwaltet:

1. Systemzugriff
2. Dateizugriff
3. Fachanwendungszugriff

Onboarding

1. Systemzugriff

Der Systemzugriff wird auf Servern verwaltet.

Benutzer: Benutzer erhalten vom IT-Bereich ein Benutzerkonto und ein Kennwort und haben damit grundsätzlichen Zugang zum IT-System.

Geräte: Geräte werden vom IT-Bereich in das System integriert.

2. Dateizugriff

Sämtliche Benutzer erhalten vom IT-Bereich Zugriff auf alle Dateien der Organisation. Ausgenommen sind die besonderen Sicherheitsbereiche

- Leitung
- Superintendenturen
- Personalabteilung

Hier haben nur die jeweilig zugeordneten Mitarbeiter Zugriff auf die Daten.

3. Fachanwendungszugriff

Die Verwaltung der Berechtigungen auf Fachanwendungen erfolgt je nach Programm im IT-Bereich oder in der Fachabteilung.

Offboarding

Soweit die Information zum IT-Bereich gelangt, werden nach Beschäftigungsende die o.g. Zugriffsrechte entzogen und Konten, ggf. erst nach einer bestimmten Frist, entfernt.

Datensicherung

Die Datensicherung für den Bereich Duisburg umfasst die Dateien auf den Netzwerklaufrwerken und Fachanwendungsdaten der lokal zur Verfügung gestellten Fachanwendungen. Die Daten werden täglich auf Datensicherungsbändern in Form einer Komplettsicherung gesichert. In der Folgeweche werden die Daten von Montag bis Donnerstag überschrieben. Die Sicherung am Freitag wird für 10 Wochen aufbewahrt und erst in der 11. Woche wieder überschrieben.

In unregelmäßigen Abständen erfolgt eine Überprüfung der Sicherung.

Die Datensicherungsbänder werden im Serverraum gelagert. Hier gäbe es Optimierungsbedarf, die Bänder an einem entfernten Ort zu lagern. Praktische Umsetzung aber schwierig.

Die Datensicherung für den Bereich Dinslaken erfolgt über den Dienstleister über Cloudsicherung.

Die Datensicherung der von Externen angebotenen Fachanwendungen erfolgt durch den jeweiligen Anbieter.

Schulung und Awareness

Schulungen finden unregelmäßig nach Bedarf statt. In der Regel werden neue Mitarbeiter durch Kollegen in der Anwendung der Fachprogramme geschult. Kenntnisse in Office-Programmen sind Einstellungsvoraussetzung, weshalb keine Schulungen zu Office-Programmen angeboten werden.

Awareness-Schulungen sind Teil des IT-Sicherheitskonzeptes. Sie sollen regelmäßig stattfinden, fanden aber seit Einführung des IT-Sicherheitskonzepts erst ein Mal statt. Optimierungsbedarf.

Datenklassifizierung und -schutz

Regelungen zur Datenklassifizierung sind Teil des IT-Sicherheitskonzepts. Die Regelung wird Stand 2025 noch nicht praktiziert (öffentlich, vertraulich, streng geheim etc.).

Zum Datenschutz gibt es ein gesondertes Datenschutzkonzept.