Anwenden und Betreiben von Applikationen IKS Prozess Nr. 011

1 Zweck

Die Benutzerverwaltung für die Schulverwaltungssoftware erfolgt korrekt.
Die Anwendung und der Betrieb IKS relevanter Applikationen sind unter Berücksichtigung von Sicherheitsaspekten gewährleistet
Hinweis: Die Rubrik „Dezentraler Applikationsbetrieb“ ist nur anwendbar, falls an der Schule dezentral betriebene IKS relevante Applikationen bestehen

2 Geltungsbereich

Alle IT-Applikationen der TBZ

3 Weiter geltende Unterlagen

- Benutzerliste
- Zutrittsberechtigungskonzept/Schliesskonzept
- Passwortempfehlungen gem. Melde- und Analysestelle Informationssicherung (Melanie)

4 Richtlinien

4.1 Schulverwaltungs-Software/Benutzerverwaltung

Für den Betrieb ist die Abteilung IT des MBA verantwortlich.

- Der Rektor/die Rektorin ist verantwortlich, dass Benutzer/innen in der Schulverwaltungssoftware erfasst / mutiert /deaktiviert werden
  - Lehrpersonen: erfassen/mutieren auf Basis der Anstellungsverfügung[1],
    deaktivieren bei Auslauf der Anstellungsverfügung[1]
    [1]Hinweis: Ein Benutzer/eine Benutzerin kann vor Erhalt der Verfügung auf Basis eines Auftrags durch den Rektor/die Rektorin eröffnet werden. Erhalt der Verfügung spätestens 3 Monate nach der Erfassung des Benutzers/der Benutzerin muss geprüft werden in der jährlichen Überprüfung der Benutzerlisten
  - Lernende: erfassen/mutieren auf Basis Lehrvertrag im KOMPASS,
    deaktivieren bei Auslauf des Lehrvertrags
  - Verwaltungspersonal: erfassen/mutieren/deaktivieren durch die/den Personalverantwortliche/n
    Verwaltungspersonal schriftlich bei der Informatikabteilung MBA beantragen

- Benutzerlisten sind jährlich auf Vollständigkeit und Richtigkeit zu überprüfen, von Rektor/in genehmigen zu lassen und abzulegen

4.2 Dezentraler Applikationsbetrieb/Allgemeine Anforderungen

- Der Rektor/die Rektorin ist verantwortlich, dass lokale/r Administrator/in definiert und dokumentiert ist
- Der Rektor/die Rektorin genehmig und dokumentiert die Stellvertretung des lokalen Administrators/der Administratorin

- Der Rektor/die Rektorin regelt den Zutritt zu den Räumlichkeiten mit Informatik-Infrastruktur (z.B. Serverraum) durch das Schliesskonzept
- Der Rektor regelt die Abgabe von Schlüsseln mit Zutrittsberechtigung zu Räumlichkeiten mit Informatik -Infrastruktur und dokumentiert diese nachvollziehbar (z.B. mit Schlüsselliste)
- Der Rektor/die Rektorin überprüft, visiert und dokumentiert die Zutrittsberechtigungen jährlich
- Der Rektor/die Rektorin stellt sicher, dass bei Mitarbeitenden jährlich Sensibilisierungsmassnahmen für die Passwortwahl durchführt werden
- Der Rektor/die Rektorin protokolliert und dokumentiert die durchgeführten Sensibilisierungsmassnahmen
- Der/die lokale Administrator/in ist verantwortlich, dass regelmässig Backups durchführt werden
- Der Lokale Administrator ist verantwortlich, dass Backup-Protokolle bis zum nächsten Jahresbackup (elektronisch) archiviert werden

4.3 Personendaten

Personendaten dürfen wegen der Informationssicherheit nur verschlüsselt und via Webtransfer an berechtigte Personen übermittelt werden

5 Output

- Archivierte Benutzerlisten
- Archivierte Backup-Protokolle
- Protokollierte Sensibilisierungsmassnahmen

6 Qualitätsziele

- Die Informationssicherheit der wesentlichen IT-Applikationen ist sichergestellt
- Der Zugriff auf Personendaten ist auf einen kleinen Kreis von Verwaltungsmitarbeitenden beschränkt
- Personendaten dürfen nur mit Bewilligung des Rektors/der Rektorin an Drittpersonen weitergegeben werden

7 Verteiler

Admin: A; SL:I

Verfasser/in: R. Meier, Rechnungsführerin, E. Schwyter, Rektor

Genehmigt: E. Schwyter, Rektor