Merkblatt für die Nutzung der zentralen Schulverwaltungsumgebung (ZSVU)

Dieses Papier fasst die Hinweise für die datenschutzkonforme Nutzung der zentralen Schulverwaltungsumgebung (ZSVU) zusammen. Die ZSVU wird den Berliner Schulen durch die Senatsverwaltung für Bildung als zentrales IT-System für Verwaltungsaufgaben zur Verfügung gestellt.

Wartung und Pflege des IT-Systems erfolgt durch das IT-Dienstleistungszentrum Berlin (ITDZ).

Ansprechpartner für den Support (Hardware und Software) ist das **Schulservicezentrum Berlin** (SSZB): **sszb@schule.berlin.de**, Telefon **030 9021-4666**

Nutzungsberechtigte des rollenbasierten IT-Verwaltungssystems sind die staatlichen Beschäftigten der Schule, die mit (Kern-)Verwaltungsaufgaben beauftragt wurden. Es gibt verschiedene Rollen:

Die Schulleitung

- hat Zugriff auf alle Ordner und Dateien des gesamten Systems (mit Ausnahme des persönlichen Ordners anderer Nutzungsberechtigter) und auf einen persönlichen Ordner,
- legt fest, welche Beschäftigten einen Zugang erhalten sowie deren Rechte (Zugriffsrechte auf Funktionsordner, USB-Port-Freischaltung und Funktions-E-Mail-Adresse).

Andere Nutzungsberechtigte

- haben durch die Schulleitung zugewiesene Rollen (zum Beispiel Sekretariat, Koordination, Sonderpädagogik). Dieses Rollensystem ist – *wie im Migrationsgespräch mit der Schulleitung abgestimmt* – darauf ausgerichtet, die Struktur der Schule abzubilden.
- haben alleinigen Zugriff auf ihren persönlichen Ordner (Homeverzeichnis),
- haben Zugriff auf Funktionsordner entsprechend der durch die Schulleitung festgelegten Rolle.

Die Schulleitung entscheidet darüber, ob und wann neue Benutzerkonten angelegt bzw. gelöscht oder Rechte geändert werden. Die Anforderung übermittelt die Schulleitung per signierter E-Mail von <BSN@BSN.schule.berlin.de> an das SSZB (sszb@schule.berlin.de).

Die Nutzungsberechtigten sind zur Einhaltung der folgenden Vorgaben verpflichtet.

1. Die Nutzung der ZSVU dient ausschließlich dienstlichen Zwecken.
2. Das Benutzerkonto ist personengebunden. **Eine Weitergabe der Zugangsdaten ist unzulässig.** Halten Sie ihr Passwort geheim.

   Das gilt auch für den Vertretungsfall. Im Vertretungsfall beauftragt die Schulleitung ein neues Benutzerkonto per signierter E-Mail beim SSZB. Das Konto wird vom SSZB in kurzer Zeit eingerichtet.

   Bei Verdacht auf Missbrauch informieren Sie bitte sofort das SSZB. Das SSZB kann Konten sperren.
3. Auf die persönlichen Ordner haben die Nutzungsberechtigten jeweils nur selbst Zugriff. Speichern Sie schulrelevante Daten in Funktionsordnern, um im Vertretungsfall Zugriff auf diese Daten zu gewähren.

   Bei der Schulleitung erfahren Sie, welche Beschäftigten auf welche Funktionsordner Zugriff haben.
4. Achten Sie bei der Benutzung des Systems auf IT-Sicherheitsregeln.
   - Öffnen Sie Anhänge von E-Mails nur, wenn der Absender vertrauenswürdig ist und der Anhang abgesprochen ist, um nicht Opfer von gefälschten E-Mails zu werden.
   - USB-Sticks sind häufige Ursache für den Befall mit Schadsoftware, weshalb nur Personen eine USB-Port-Freischaltung erhalten sollen, die sie für ihre Arbeit benötigen. Wenn Sie eine Berechtigung besitzen, verwenden Sie diese stets verantwortungsvoll und nutzen Sie beispielsweise nur Sticks, die hundertprozentig vertrauenswürdig sind.
   - Bitte melden Sie Unregelmäßigkeiten sofort dem SSZB.
   - Aktivieren Sie die Bildschirmsperre bei Verlassen des Raumes.
   - Weitere Hinweise finden Sie im IT-Sicherheitshandbuch[1].
5. Beachten Sie die Rechtmäßigkeit bei der Weitergabe von Daten (Ausdruck, E-Mailen, Speichern auf Datenträgern). Wenn Lehrkräfte personenbezogene Daten auf privaten Geräten verarbeiten, müssen sie dies zuvor bei der Schulleitung beantragen und sich zur Einhaltung der datenschutzrechtlichen Vorgaben verpflichten.[2]
6. Benutzen Sie für Daten der Schulverwaltung keine Speicherdienste im Internet (Cloud). Dafür dient die ZSVU.
7. Versenden Sie vertrauliche Daten per E-Mail stets mit dem durch die Senatsverwaltung zur Verfügung gestellten Verschlüsselungszertifikat. Mit einer signierten Mail wird die Identität des Absenders bestätigt. Dies kann eine erforderliche Unterschrift ersetzen.
8. Wechselt ein Nutzer die Schule oder scheidet aus dem Dienst aus, so ist das dem SSZB anzuzeigen, damit der Zugang zur ZSVU gesperrt bzw. geändert werden kann. Zuvor ist mit diesem Nutzer zu klären, ob Daten aus dem persönlichen Ordner gesichert wurden.

Bei Fragen stehen Ihnen die Regionalen Datenschutzbeauftragten gern zur Verfügung.

[1] IT-Sicherheitshandbuch für die Verwaltungen in Berliner Schulen, Version 2.1
https://www.egovschool-berlin.de/IT-Sicherheit-Grundlagen
[2] § 64 BlnSchulG, § 12 SchuldatenVO (Antrag unter https://www.egovschool-berlin.de/vorlagen)