Benutzerhinweise zur Informationssicherheit und zum Datenschutz

Teil der technisch-organisatorischen Maßnahmen im Rahmen des Betriebs von BOLLE (oder ähnlichen Systemen) sind **regelmäßige Sensibilisierungsmaßnahmen des Personals**. Das Schulpersonal muss darüber informiert werden, wie es sich im Falle des Verlustes von Zugangsdaten zu verhalten hat. Die Schulleitungen oder die schulischen Beauftragten für Datenschutz geben jährlich Hinweise zur Informationssicherheit und zum Datenschutz. Die Benutzerhinweise auf dieser Seite können dabei behilflich sein.

Inhalt

1. Allgemeines

Sie verwalten über BOLLE personenbezogene Daten der Schüler:innen. Seien Sie sich stets der Tatsache bewusst, dass die Vertraulichkeit der Daten und ihr Schutz vor unbefugter Veränderung höchste Priorität hat und in Ihrer Verantwortung liegt.

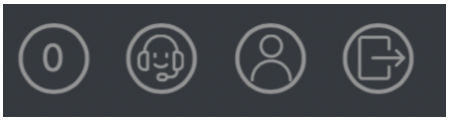
Der Zugang zu BOLLE wird daher durch eine Zwei-Faktor-Authentisierung besonders gesichert. Ihr Benutzerkonto wird sowohl durch ein persönliches Passwort als auch einen weiteren Faktor geschützt. Der weitere Faktor kann

- die Key-Datei bzw.
- die Verwaltungskey-Datei,
- ein zusätzliches zeitlich limitiertes Einmalkennwort (TOTP) oder

- die Identifikation mit einem bestimmten, bereits als vertrauenswürdig definierten Gerät sein.

Sowohl beim Passwort als auch bei den zweiten Faktoren sollen folgende sicherheitsrelevante Aspekte beachtet werden.

Die wichtigste Regel: **Immer ordentlich ausloggen!**
Klicken Sie dafür auf das Logout-Symbol ganz oben rechts.



Ähnlich wie bei anderen sensiblen Bereichen im Internet (z.B. Online-Banking) erfolgt bei BOLLE ein automatischer Logout. Sollten Nutzer:innen aus welchen Gründen auch immer den oben beschrieben ordentlichen Logout vergessen, werden sie innerhalb eines kurzen Zeitfensters automatisch ausgeloggt. Vor einem **automatischen Logout** wird man in der Menüleiste mit einem roten Countdown informiert. Wenn man auf den Countdown klickt oder eine andere Aktion innerhalb von BOLLE ausführt, wird das Zeitfenster zum automatischen Logout zurückgesetzt.

2. Passwort

- je länger, desto besser: Passwortlänge von **mindestens zehn Zeichen** wählen
- es **müssen** Groß- **und** Kleinbuchstaben verwenden werden
- das **Passwort muss eine Zahl oder ein Sonderzeichen** enthalten
- **erlaubte Sonderzeichen sind: !$%&=+#-_.:,@**
- mehrere Ziffern hinzufügen, wird empfohlen
- keine Passwort-Kombinationen, die Geburtstage (o.Ä.) enthalten
- keine Wiederholungs- und Tastaturmuster (asdf, 1234, 777)
- kein simples Passwort, das nur um ein Sonderzeichen am Wortanfang oder -ende ergänzt ist (z.B.: "!Passwort")
- nicht an andere Personen weitergeben
- nie per E-Mail versenden
- nicht auf PCs speichern, auf denen sich auch andere Menschen einloggen können
- nicht unverschlüsselt auf dem PC ablegen
- falls gespeichert, darf sich das Passwort nicht kontrolllos automatisch ausfüllen lassen
- nicht auf dem berühmten Notizzettel am Bildschirm schreiben

Weitere Informationen finden Sie beim Bundesamt für Sicherheit und Informationstechnik

bei Verlust oder Diebstahl:
Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen

Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können Sie Ihr Passwort selbst verändern.

3. Key-Datei

- nie per E-Mail versenden
- nicht an andere Personen weitergeben
- nicht vervielfältigen
- auf einem verschlüsselten mobilen Datenträger aufbewahren

Die Key-Datei wird Ihnen von Ihrem Admin vor Ort ausgestellt.

bei Verlust oder Diebstahl:
Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können Sie Ihre Key-Datei invalidieren oder sogar den Account vorerst komplett sperren.

4. Verwaltungskey-Datei

- nie per E-Mail versenden
- nicht an andere Personen weitergeben
- nicht vervielfältigen
- getrennt von der Key-Datei aufbewahren
- im besten Fall nur auf dem passwortgeschützten und verschlossenen stationären Dienstrechner ablegen und verwenden

Die Verwaltungskey-Datei ist nötig, um besonders sensible und weitreichende Bereiche in BOLLE einzusehen. Ihr Admin informiert Sie darüber, ob Sie solch einen Verwaltungskey benötigen.

bei Verlust oder Diebstahl:
Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können Sie Ihre Key-Datei invalidieren oder sogar den Account vorerst komplett sperren.

5. Zeitlich limitiertes Einmalkennwort (TOTP)

- nur auf einem persönlichen Gerät verwenden, bei dem weitere Sicherheitsmerkmale den Zugriff kontrollieren (z.B. Kennwort am Smartphone)
- nur Sie sollten Zugriff auf das persönliche Gerät haben, auf dem das TOTP ausgegeben wird

Wie Sie ein TOTP einrichten, wird Ihnen hier erklärt.

bei Verlust oder Diebstahl:
Melden Sie sich bei Ihrem schulinternen Admin. Falls Sie sich noch einloggen können, gehen Sie auf Ihr Profil (ganz oben rechts, Profilicon) und klicken links auf *Sicherheit*. Hier können Sie Ihre Zwei-Faktor-Authentisierung mittels TOTP löschen oder sogar Ihren Account sperren.

6. FIDO2

Mehr zu FIDO2 erfahren Sie auf dieser Seite.

7. Vertrauenswürdige Geräte

- sind nur Geräte, die sich permanent in Ihrem Besitz bzw. sich in Ihrer dauerhaften Zugriffskontrolle befinden
- Computer, auf denen sich auch andere Personen einloggen könnten, sind keine vertrauenswürdigen Geräte (z.B. der PC im Klassenraum oder Kolleg:innenzimmer)
- der Zugang zu vertrauenswürdigen Geräten ist abermals passwortgesichert
- Bildschirmschoner mit Kennwort sichern
- nicht unbeaufsichtigt lassen; vor allem nicht nach einer Anmeldung am Gerät

Auf vertrauenswürdigen Geräten können Sie z.B. einen FIDO2-Zugang einrichten. Mehr zu FIDO erfahren Sie hier: Allgemeines

Informationen für den Admin der Schule

Einstellungsmöglichkeiten für das Personal

bei Verlust oder Diebstahl:
Melden Sie sich bei Ihrem schulinternen Admin. Die Admins können auch Ihre FIDO2-Zugänge deaktivieren. Sie selber können sich, falls Sie sich noch einloggen können, Ihren gesamten Account oder z.B. nur die Keydatei deaktivieren. Ihre Admins können dann Ihren Account wieder aktivieren oder Ihnen einen neue Keydatei ausstellen.

Version #10
Erstellt: 11 September 2021 09:25:06 von BOLLE Support
Zuletzt aktualisiert: 7 Dezember 2023 12:38:59 von BOLLE Support