



## FÜR NUTZER: Passwortrichtlinie DSBcontrol

Sehr geehrte Kunden,

im Nachgang eines Cyberangriffs auf unseren Rechenzentrumsbetreiber wurden unsere Systeme, auf denen die Services des Digitalen Schwarzen Bretts®, der DSBmobile®-App und der Mediaboxen gehostet werden, erfolgreich entschlüsselt. Die Datenbank sowie alle Kundendaten konnten wiederhergestellt werden und wurden in eine neue Infrastruktur übertragen. Um die bestmögliche Sicherheit nach der Wiederinbetriebnahme gewährleisten zu können, ist es notwendig, ein neues Passwort für Ihren DSBcontrol-Account festzulegen.

Wir empfehlen Ihnen, die folgenden Aspekte bei der Passwortvergabe zu beachten.

### 1. Passwort ändern

Nach dem ersten Login in DSBcontrol werden Sie dazu aufgefordert, Ihr altes Passwort unverzüglich durch ein neues zu ersetzen. Befolgen Sie dafür die folgenden Schritte:

- Klicken Sie im Portal oben rechts auf Ihren Account-Namen
- Klicken Sie im Dropdown-Menü auf „Mein Account“
- Klicken Sie auf „Passwort ändern“
- Geben Sie Ihr altes Passwort ein
- Vergeben Sie ein neues Passwort
- Geben Sie Ihr neues Passwort erneut ein
- Klicken Sie unten rechts auf „Speichern“

Hier können Sie Ihre persönlichen Informationen bearbeiten. Bitte kontrollieren Sie diese Daten regelmäßig und passen Sie diese ggf. an.

**Persönliche Informationen**

Anrede: \*

Vorname: \*  Nachname: \*

Tel. Nr.: \*  E-Mail: \*

Sie haben hier die Möglichkeit ihr persönliches Passwort zu ändern. Wir empfehlen Ihnen, dies in regelmäßigen Abständen zu tun.

**Passwort: [Passwort nicht ändern](#)**

Altes Passwort:

Neues Passwort:

Passwort wiederholen:

**Das Passwort muss folgende Kriterien erfüllen:**  
Buchstaben, mindestens: 7  
Ziffern, mindestens: 2  
Sonderzeichen, mindestens: 1

**Portaleinstellungen**

Sprache:

Mediathek:

Gültigkeit von Spots und News automatisch begrenzen

Newsgültigkeit:

Spotgültigkeit:

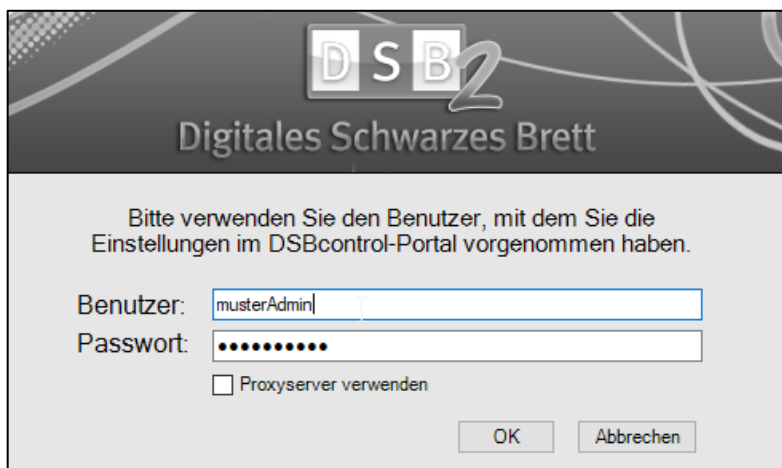
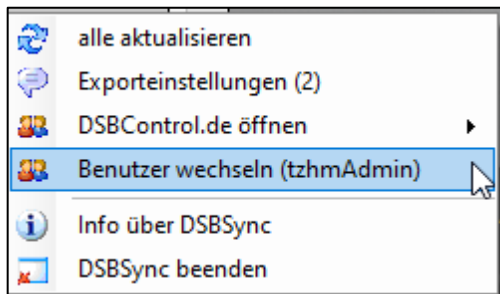
## 2. Passwort wählen

Bei der Vergabe Ihres neuen, individuellen Passworts sollten die folgenden Kriterien erfüllt werden:

- Bereits benutzte Passwörter nach einem Passwortwechsel nicht wiederverwenden
- Mindestens 10 Zeichen lang, davon min. 7 Groß- und Kleinbuchstaben, 2 Ziffern und ein Sonderzeichen (z.B. \*§\$%&)
- Nicht mehr als ein aufeinanderfolgendes identisches Zeichen
- Keine Trivialpasswörter, dazu gehören aufeinanderfolgende Buchstaben und Zahlen, z. B. 123456 oder abcdefg oder aufeinanderfolgende Tastaturzeichen, z.B. asdfgh
- Das Passwort sollte nicht mit dem einzelnen Nutzer in Verbindung gebracht werden können, z. B. Name, Wohnort, Kfz-Kennzeichen
- Keine Namen/Begriffe, die in Wörterbüchern stehen können
- Die Benutzerkennung sollte nicht Bestandteil des Passworts sein
- Das Passwort sollte nicht in anderen Umgebungen (z.B. im Internet, auf Portalen etc.) gleichlautend verwendet werden

### 3. Passwort in DSBSync ändern

Sollten Sie die Erweiterung DSBSync nutzen, ist es notwendig, auch hier Ihr neues Passwort einzustellen. Dies betrifft sowohl die Desktop-Anwendung als auch den ggf. installierten Windowsdienst. DSBSync ist erst dann wieder verfügbar, wenn Sie ein neues Passwort in DSBcontrol festlegt und in DSBSync hinterlegt haben. **Bitte beachten Sie, dass DSBSync aus technischen Gründen erst am Mittwoch, den 21. Juni 2023, wieder zur Verfügung steht.**



### 4. Passwort vertraulich behandeln

Das Passwort sollte vertraulich behandelt und geheim gehalten werden, sodass es Dritten nicht zugänglich ist. Es sollte ebenso nicht in Dateien oder Skripten gespeichert und auch nicht am Arbeitsplatz, z.B. auf Zetteln, hinterlegt oder auf Funktionstasten gespeichert werden. Sollten Sie den Verdacht auf den Verlust der Vertraulichkeit oder Ausspähung haben, sollte das Passwort sofort zurückgesetzt werden. Kontaktieren Sie dazu den DSBcontrol-Admin Ihrer Bildungseinrichtung bzw. Ihres Unternehmens oder den heinekingmedia Support unter <https://heinekingmedia.atlassian.net/servicedesk/customer/portal/5>. Schalten Sie bei Verdacht auf Missbrauch auch Ihre IT-Abteilung ein. Um eine Kenntnisnahme durch Unbefugte zu verhindern, empfehlen wir Ihnen, Ihr Passwort verdeckt einzugeben. Die Anmeldung sollte niemals unter einem fremden Benutzernamen/Passwort erfolgen.

Vielen Dank für Ihr Verständnis und Ihre Mithilfe.