# Hinweise zum Umgang mit Passwörtern

Vom 10. Januar 2025

**Stand 10.01.2025**

„Gute Passwörter sind das Eingangstor zur Informationssicherheit."

Ein nicht zu unterschätzendes Sicherheitsrisiko stellen die von den Anwenderinnen und Anwendern genutzten Passwörter dar. Untersuchungen haben gezeigt, dass einfache Passwortvarianten bevorzugt werden, wie „123456789", „hallo", „password", „iloveyou", „qwerty123"[1] oder einfach der eigene Name, der des Haustieres oder das Geburtsdatum. Diese Passwortvarianten stehen ganz oben auf Listen von Hackern. Damit wird es Hackern leicht gemacht, Passwörter zu erraten, indem sie vollautomatisch ganze Wörterbücher für den Angriff mit Hochleistungs-PCs durchprobieren.

Auch kommt es immer wieder vor, dass Kolleginnen und Kollegen oder Vorgesetzte die Benutzerkennung und das Passwort für Vertretungszwecke erhalten oder dass mehrere Mitarbeitende für ein DV-Programm eine gemeinsame Benutzerkennung und ein gemeinsames Passwort verwenden. Datenschutzrechtlich sind beide Varianten nicht zulässig, denn durch das Passwort wird nachgewiesen, dass es sich um diejenige Person handelt, die das Passwort kennt.

**Das bedeutet, durch die Weitergabe eines Passworts kann eine andere Person in Ihrem Namen handeln und der Gegenbeweis fällt dann schwer.**

Deshalb erfüllt nur die Vergabe individueller Benutzerkennungen und individueller Passwörter die Anforderungen des Datenschutzrechts.

**Damit Passwörtern ihre wichtige Funktion und ein hoher Schutz zukommen, sind starke Passwörter zu verwenden. Die Passwörter sind immer geheim zu halten!**

Folgende Hinweise zum Umgang mit Benutzerkennungen und Passwörtern sind zu beachten:

1. Es sind **individuelle Benutzerkennungen** und **individuelle Passwörter** zu verwenden.
2. Ein gutes Passwort muss **mindestens 12 Zeichen** lang sein.
3. Es **muss** Zeichen aus mindestens drei der folgenden Kategorien enthalten: Großbuchstaben (A bis Z) und Kleinbuchstaben (a bis z), Ziffern (0 bis 9) sowie nichtalphabetische Zeichen (z. B.: !, $, #, %).
4. **Triviale Passwörter sind zu vermeiden.** Nicht verwendet werden sollten Namen von Familienmitgliedern, des Haustieres, der besten Freundin, des Lieblingsstars oder

**1** Auszug aus den meist genutzten Passwörtern in Deutschland 2023 (Quelle Hasso-Plattner-Institut).

Geburtsdaten usw. Diese Art von Passwörtern kann durch *Social Engeneering* durch einen Unbefugten zu leicht ermittelt werden.

5. Das Passwort sollte **nicht in einem Wörterbuch vorkommen.** Zu vermeiden sind auch gängige Varianten oder Wiederholungs- oder Tastaturmuster, also nicht „asdfgh“ oder „1234abcd“ usw.
6. Das Passwort sollte nicht mehr als zwei aufeinanderfolgende Zeichen des vollständigen Namens des Benutzers enthalten.
7. Für ein **gutes Passwort** lohnt es sich, kreativ zu werden. Um ein komplexes und dennoch leicht zu merkendes Passwort zu konstruieren, empfiehlt sich ein Merksatz als Eselsbrücke. Dabei denken Sie sich einen Satz aus und benutzt von jedem Wort beispielsweise nur den ersten Buchstaben. Anschließend verwandeln Sie bestimmte Buchstaben in Ziffern oder Sonderzeichen.

   So wird z. B. aus dem Merksatz „Zum Datenschutz gehört ein gutes Passwort, um unberechtigte Zugriffe zu verhindern!“ das Passwort „ZDg1gP@uuZz8!“.
8. **Passwörter sollen sich nicht wiederholen.** Daher sollte keines der letzten 10 Passwörter für ein DV-Programm oder IT-System erneut genutzt werden.
9. **Passwörter sollen nicht mehr regelmäßig geändert werden.** Sie sollten innerhalb eines Jahres nur eine Änderung des Passwortes durchzuführen. Für mehrere DV-Programme oder IT-Systeme sind unterschiedliche Passwörter zu verwenden. Problematisch ist die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke zu verwenden. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, sind auch die anderen Anwendungen nicht mehr geschützt. Verwenden Sie statt dessen besser mehrere Varianten eines Passworts „ZDg1gP@uuZz8!_dienst1“, „ZDg1gP@uuZz8!_dienst2“, „ZDg1gP@uuZz8!_dienst3“, usw.
10. **Voreingestellte Passwörter in DV-Programmen sind zu ändern.** Bei vielen DV-Produkten werden bei der Installation oder im Auslieferungszustand in den Accounts leere Passwörter oder allgemein bekannte Passwörter („0000“) verwendet. Diese müssen Sie umgehend ändern.
11. Hat die IT-Administration Ihnen ein Passwort eingerichtet, so haben Sie dieses **„Start-Passwort“** bei der ersten Anmeldung zu ändern.
12. Lassen Sie sich beim **Eintippen des Passworts nicht über die Schulter schauen**.
13. **Teilen Sie niemals Dritten** (auch nicht den IT-Administratorinnen und Administatoren) **ihr Passwort mit**. IT-Administratorinnen und Administratoren haben grundsätzlich alle für Ihre Arbeit notwendigen Rechte und sind nicht auf die Mitteilung Ihres Passwortes angewiesen.
14. Bei Abwesenheit ist der **Bildschirmschoner** zu starten und **mit Kennwort** zu sichern. Bei den gängigen Betriebssystemen haben Sie zusätzlich die Möglichkeit, den Bild-

schirm nach einer gewissen Zeit der Inaktivität automatisch sperren zu lassen. Die Entsperrung erfolgt erst nach Eingabe des korrekten Passwortes. Damit wird verhindert, dass Dritte sonst bei vorübergehender Abwesenheit Zugang zum PC, den DV-Programmen und Daten erhalten.

15. **Passwörter sollten niemals per Zettel am Bildschirm oder auf dem Schreibtisch kleben oder unter der Tastatur liegen oder unverschlüsselt auf dem PC abgelegt werden.** Für die Hinterlegung im Notfall darf ein Passwort nur schriftlich und sicher aufbewahrt werden, d. h. in einem verschlossenen Kuvert mit Datum und Unterschrift, welches unter Verschluss gehalten werden muss. Diese Ausnahme ist schriftlich bei der Dienststellenleitung zu beantragen.
16. Falls eine **Mehr-Faktor-Authentifizierung (MFA)** möglich ist, ist diese zu nutzen!

Sie können Passwörter auch auf dem Rechner in einer verschlüsselten Datei ablegen. Fragen Sie ggf. Ihre IT-Administration nach einem Passwort-Manager, wie z. B. *Bitwarden* oder *KeePass*. Diese Programme können neben der Passwort-Verwaltung auch starke Passwörter unter Berücksichtigung der o. a. Hinweise generieren. Das hat den Vorteil für Sie, dass Sie sich nur noch ein gutes Masterpasswort überlegen und merken müssen. Funktionen oder Plug-Ins zum Synchronisieren von Passwörtern über Onlinedienste Dritter oder die anderweitig an Dritte übertragen werden, sind zu deaktivieren.

**Ein Kennwort ist umgehend zu ändern**, wenn der Verdacht besteht, dass es einem Dritten bekannt wurde. In diesem Fall ist die Dienstellenleitung und die oder der **IT-Sicherheitsbeauftragte** unverzüglich über den Sicherheitsvorfall zu informieren.

Beispiele:

- Eine andere Person hat Ihnen bei der Eingabe Ihres Passworts zugesehen (*Shoulder Surfing*).
- Sie haben das Passwort weitergeben müssen, da ein Stellvertreterzugriff nicht eingerichtet werden konnte.
- Ihre Zugangsdaten sind bei *Have I been pawned* oder auch beim *Identity Leak Checker* des HPI als kompromittiert gemeldet worden.

**Hinweise für die IT-Administration:**

1. Die Einstellungen des DV-Programms sollten vorsehen, dass nach mehreren fehlerhaften Anmeldeversuchen unter derselben Benutzerkennung diese für die weitere Benutzung gesperrt wird.
2. Um zu verhindern, dass die Benutzerin oder der Benutzer das gleiche Passwort beim Wechsel direkt wieder einstellt oder zwei oder mehr Passwörter im Wechsel nutzt, sollte system- bzw. programmseitig eine Passworthistorie mit mindestens den letzten zehn benutzten Passwörtern aktiviert sein.

3. System- oder programmseitig sollten möglichst Trivialpasswörter erkannt und abgelehnt werden. Die Liste von Trivialpasswörtern ist regelmäßig zu ergänzen.
4. Passwörter für administrative Einsätze sollten eine Länge von mindestens 20 Zeichen aufweisen. Idealerweise sollten solche Passwörter eine Mindestlänge von aktuell 64 Zeichen haben. Hierbei dürfen durchaus ganze Sätze zum Einsatz kommen, solange es sich nicht um bekannte Redewendungen oder Zitate handelt.