

# Passwörter sicher verwalten

## MENSCH

### ✓ Richtig vorbeugen

- Einzigartiges, langes Passwort (mind. 12 Zeichen) für jeden Dienst verwenden.
- Passwort-Manager unternehmensweit einsetzen, statt Passwörter zu merken oder zu notieren.
- Zwei-Faktor-Authentifizierung überall aktivieren, wo verfügbar.
- Passwörter niemals per E-Mail, Chat oder auf Zetteln weitergeben.
- Keine persönlichen Informationen (Namen, Geburtsdaten) in Passwörtern verwenden.
- Regelmäßiger, aber nicht übertriebener Passwortwechsel bei sensiblen Konten.

### ■ Im Ernstfall – Schritt für Schritt

**Vorfall-Protokoll** (bitte ausfüllen)

|                                    |  |
|------------------------------------|--|
| Datum:                             |  |
| Uhrzeit:                           |  |
| Betroffenes System / Gerät:        |  |
| Gemeldet durch:                    |  |
| Gemeldet an (IT-Verantwortlicher): |  |

- 1. Passwort sofort ändern – von einem sauberen, vertrauenswürdigen Gerät aus.
- 2. Gleiches Passwort auf anderen Diensten genutzt? Dort ebenfalls sofort ändern.
- 3. Zwei-Faktor-Authentifizierung aktivieren, falls noch nicht geschehen.
- 4. Konto auf verdächtige Aktivitäten/Anmeldungen prüfen.
- 5. IT-Abteilung informieren, insbesondere bei Firmenkonten.
- 6. Betroffene Kolleg\*innen/Kunden informieren, falls Daten gefährdet waren.