PASSWÖRTER

Richtlinie Passörter

Warum diese Richtlinie?

Passwörter sind äußerst wertvoll und ein beliebtes Ziel für Hacker. Die Hauptursache für die meisten Hacker-Angriffe sind gestohlene oder schwache Passwörter. Eine wichtige Verteidigungslinie und ein unschätzbarer Aspekt unserer Unternehmenssicherheit sind unsere Mitarbeiterinnen und Mitarbeiter.

Die Sensibilisierung unserer Mitarbeitenden für die Gefahren, die von Cyber-Kriminellen ausgehen, ist uns wichtig. Dazu gehört auch, eine intelligente und konsequente Passwortpolitik zu entwickeln und durchzusetzen.

Um uns angesichts der rasanten Entwicklung von Cyber-Angriffen bestmöglich zu schützen, haben wir eine umfassende Passwort-Richtlinie entwickelt. Diese Richtlinie ist für alle Mitarbeiterinnen und Mitarbeiter des Unternehmens verbindlich.

Absolute Vertraulichkeit ist immer zu beachten. Passwörter dürfen mit niemandem geteilt werden. Dies gilt auch für die IT-Abteilung. Sie dürfen nicht per E-Mail, Telefon oder auf andere Weise weitergegeben werden. Auf keinen Fall dürfen sie aufgeschrieben werden. Es empfiehlt sich, einen sicheren elektronischen Passwortmanager zu verwenden.

RICHTLINIE

Überblick

Diese Richtlinie dient dazu, die Erstellung, die Pflege und den Schutz von Passwörtern in unserem Unternehmen effektiv zu gestalten.

Geltungsbereich

Für alle Mitarbeiterinnen und Mitarbeiter, Auftragnehmer und verbundene Unternehmen, die an unser Netzwerk angeschlossen sind oder auf Daten unseres Unternehmens zugreifen oder diese verarbeiten, gilt diese Richtlinie ausnahmslos. Sie regelt den zulässigen Umgang mit Passwörtern auf allen Systemen.

Richtlinie

Erstellung von Passwörtern

- Alle Passwörter, sowohl für Benutzer als auch für Administratoren müssen mindestens 12 Zeichen lang sein. Es wird dringend empfohlen, längere Passwörter und Passphrasen zu verwenden.
- Um die Verwendung von gängigen und leicht zu knackenden Passwörtern zu vermeiden, sollten nach Möglichkeit Passwortgeneratoren verwendet werden.
- Passwörter müssen absolut eindeutig sein. Sie dürfen nicht für andere Systeme, Anwendungen oder persönliche Konten verwendet werden.
- Passwörter, die bei der Installation voreingestellt sind, müssen sofort nach Abschluss der Installation geändert werden.

RICHTLINIE

Passwort-Alterung

- Die Passwörter der Benutzer müssen alle 3 Monate geändert werden. Passwörter, die bereits einmal verwendet wurden, dürfen nicht erneut verwendet werden.
- Passwörter auf Systemebene werden alle 2 Monate geändert.

Passwortschutz

- Passwörter dürfen an niemanden weitergegeben werden (auch nicht an Mitarbeiter und Vorgesetzte). Sie dürfen nicht veröffentlicht oder elektronisch versendet werden.
- Passwörter dürfen nicht notiert oder irgendwo im Büro aufbewahrt werden.
- Bei der Konfiguration von Passwort-"Hinweisen" dürfen keine Angaben zum Passwortformat gemacht werden (z. B. ”Urlaubsort + zweiter Vorname").
- Eine unverschlüsselte Speicherung von Benutzerkennungen und Passwörtern ist nicht zulässig.
- Benutzerkennungen und Passwörter dürfen nicht Gegenstand von Skripten zum Zweck der automatischen Anmeldung sein.
- Die Verwendung der Funktion "Passwort merken" auf Webseiten und in Anwendungen ist nicht zulässig.
- Alle mobilen Geräte, die sich mit dem Unternehmensnetzwerk verbinden, müssen mit einem Passwort und/oder einer biometrischen Authentifizierung gesichert werden. Außerdem müssen sie so konfiguriert sein, dass sie nach drei Minuten Inaktivität gesperrt werden.

RICHTLINIE

Durchsetzung

Für die Einhaltung der oben genannten Richtlinien ist jeder Einzelne verantwortlich.

Wenn Sie meinen, dass Ihr Passwort kompromittiert wurde, melden Sie den Vorfall bitte unverzüglich Ihrem Vorgesetzten oder der IT-Abteilung und ändern Sie das Passwort umgehend.

RICHTLINIE