

POLICIES CHECKLISTE

- Risiken identifizieren**
- Sinn erklären**
- Verständlich**
- Umfassend**
- Workflow beachten**
- Gültig für alle Mitarbeiter**
- Mitarbeiter schulen**
- Umsetzung überprüfen**

POLICIES CHECKLISTE

Risiken identifizieren

Was muss geschützt werden und welche Risiken gibt es? Diese Fragen sollten zunächst geklärt werden.

Sinn erklären

IT-Sicherheit sollte erklärt werden, damit die Maßnahmen nicht als zusätzliche Belastung oder gar Bestrafung gesehen werden.

Verständlich

"Nicht auf Phishing Links klicken" hilft nicht weiter. Stattdessen muss erklärt werden wie man Phishing Links erkennt.

Umfassend

Nur Policies für den Umgang mit Mails aufzustellen lässt viele andere Angriffsvektoren offen.

Workflow beachten

IT-Sicherheitsmaßnahmen sollten bestmöglich in bestehende Prozesse integriert werden.

Gültig für alle Mitarbeiter

Wenn für das Top Management andere Regeln gelten dann a) sinkt die Motivation zur Umsetzung und b) wird die Policy ausgehebelt.

Mitarbeiter schulen

Jeder Mitarbeiter sollte ein Grundverständnis für typische Angriffe haben um ihnen nicht zum Opfer zu fallen.

Umsetzung überprüfen

Wird die Policy auch umgesetzt und eingehalten? Oder gibt es Schlupflöcher die zu neuen Sicherheitslücken führen?