IT-Sicherheitscheckliste

Mitarbeitende: Schwachstellenanalyse & Maßnahmen

DIGITAL AGENTUR BERLIN

Prüfen Sie an Hand der folgenden 10 Fragen, wie Ihr Unternehmen in Bezug auf IT-Sicherheit aufgestellt ist. Wenn Sie eine Frage mit **Nein** beantworten, haben wir für Sie Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1.	**Gibt es eine Stellenbeschreibung für jede*n Mitarbeiter*in?**	☐	☐	Es soll eine Stellenbeschreibung pro Mitarbeiter*in geben, in der dessen*deren Verantwortlichkeiten festgehalten sind.
2.	**Kennen die Mitarbeitenden die Vorgaben zur IT-Sicherheit?**	☐	☐	Die Leitung oder IT-Sicherheitsverantwortlichen müssen Mitarbeitenden die IT-Sicherheitsrichtlinien bekannt machen und umsetzen lassen.
3.	**Haben alle Mitarbeitenden grundlegende IT-Sicherheitskenntnisse?**	☐	☐	Alle Mitarbeitenden sollten Grundkenntnisse zur IT-Sicherheit haben bzw. mindestens für ihr berufliches Arbeitsgebiet.
4.	**Gab es für alle Mitarbeiter*innen grundlegende IT-Schulungen oder eine Awareness-Aufklärung?**	☐	☐	Alternativ durch interne oder externe Kräfte eine Schulung bzw. IT-Sicherheits-Awareness-Aufklärung durchführen lassen.
5.	**Lesen verantwortliche Mitarbeitende Fachliteratur zu IT-Sicherheit und werden Änderungen bezüglich IT-Sicherheit verfolgt und umgesetzt?**	☐	☐	Regelmäßiger (z. B. jährlicher) Check, ob es Änderungen (z. B. gesetzliche) in der IT-Sicherheit gibt.
6.	**Pflegen verantwortliche Mitarbeitende IT-Sicherheits-spezifische Kontakte?**	☐	☐	Fachspezifische Expertengruppen und -verbände sollen regelmäßig durch verantwortliche Mitarbeitende aufgesucht werden.
7.	**Gibt es einen standardisierten und umgesetzten „Onboarding-Prozess" für Mitarbeitende bezogen auf die IT-Einrichtung?**	☐	☐	› Der Onboarding-Prozess sollte einheitlich digitalisiert sein für IT-bezogene Themen, z. B. Onboarding-Checkliste in einem HR-System. › Z. B. Hardware- und Lizenzkauf, Vergabe von Berechtigungen
8.	**Gibt es einen standardisierten und implementierten „Offboarding-Prozess" für Mitarbeitende bezogen auf die IT-Einrichtung?**	☐	☐	› Der Offboarding-Prozess sollte einheitlich digitalisiert sein für IT-bezogene Themen › Z. B. IT-Rückgabeformular für Hardware und rechtzeitige Löschung von Berechtigungen
9.	**Gibt es für Verstöße von Mitarbeitenden gegen die interne IT-Sicherheit arbeitsrechtliche Sanktionen?**	☐	☐	Interne Regelungen bzgl. IT-Sicherheitsverstößen sollten den Mitarbeitenden bekannt sein, z. B. Abmahnung bei Nichtbefolgung.
10.	**Wird festgelegt, ob und welche IT-Sicherheitsvereinbarungen für den*die gekündigte*n Mitarbeiter*in weiter gelten?**	☐	☐	Verantwortlichkeiten und Vertraulichkeitspflichten, die für den*die Mitarbeiter*in nach Beendigung des Arbeitsverhältnisses gelten, müssen vereinbart werden.

Gerne unterstützen wir Sie bei der Umsetzung der Maßnahmen zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen. Wir freuen uns auf Ihre Anfrage an **info@digitalagentur.berlin**.

Weitere Informationen finden Sie auch auf **digitalagentur.berlin**.