DIGITAL AGENTUR BERLIN

IT-Sicherheitscheckliste

Mitarbeitende: Schwachstellenanalyse und Maßnahmen

Der Begriff „**Mitarbeitende**“ wird im Folgenden für alle Arbeitnehmerinnen und Arbeitnehmer, mit oder ohne Führungsverantwortung, aber auch Auszubildende oder Praktikant*innen, festangestellte oder freie Mitarbeitende und auch Leiharbeitskräfte verwendet, die in Ihrem Unternehmen an der elektronischen Datenverarbeitung beteiligt sind und die auf Ihre IT-Geräte zugreifen.

Prüfen Sie anhand 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 Beispiel-Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1. Sind im Unternehmen die Verantwortlichkeiten (für IT-Sicherheit, Buchhaltung, Finanzen etc.) benannt und bekannt?	☐	☐	Erstellung einer Übersicht mit Verantwortlichkeiten und Ansprechpartner*innen.
2. Ist ein aktuelles Rollen- und Rechtekonzept vorhanden?	☐	☐	▪ Erstellen Sie ein Konzept, welche Position (Person), welche Rechte und Rollen in den Firmensystemen haben muss. ▪ Achten Sie dabei auf das Minimalprinzip (Zugriff, nur wenn nötig) und vermeiden Sie Interessenskonflikte. ▪ Trennen Sie hierbei zwischen Administrations- und Arbeitsaccounts. ▪ Halten Sie das Konzept aktuell.

Mitarbeitende: Schwachstellen-analyse und Maßnahmen

DIGITAL AGENTUR BERLIN

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
3.	**Gibt es für die Mitarbeitenden Vorgaben zur IT-Sicherheit und sind diese bekannt?**	☐	☐	Erstellen Sie einfach umzusetzende IT-Sicherheitsrichtlinien (bspw. sichere Passworte, Umgang mit E-Mail-Anhängen, usw.), schulen Sie diese regelmäßig und/oder verpflichten Sie alle Mitarbeitenden schriftlich zur Einhaltung.
4.	**Haben insbesondere IT-Verantwortliche die Möglichkeit, sich über den Stand der Technik informiert zu halten?**	☐	☐	Stellen Sie dementsprechende zeitliche und fachliche Ressourcen zur Verfügung (Webseitenzugriffe, Fachzeitschriften, Weiterbildungsmaßnahmen).
5.	**Werden regelmäßige und bedarfsspezifische Schulungen zum Thema IT-Sicherheit durchgeführt?**	☐	☐	▪ Analog zu den Schulungen im Bereich Arbeitssicherheit und Brandschutz sind jährlich Schulungen zum Thema IT-Sicherheit für alle Mitarbeitenden durchzuführen. ▪ Neben klassischen Schulungen können auch andere Methodiken wie „Workshops“ oder „Serious Games“ angewendet werden.
6.	**Wird im Rahmen von Schulungen auch auf arbeitsrechtliche oder sogar mögliche juristische Folgen hingewiesen?**	☐	☐	Kommunizieren Sie regelmäßig interne Vorgaben bzgl. Sicherheitsverstößen an alle Mitarbeitenden, auch mit den eventuellen Folgen z. B. Abmahnung bei Nichtbefolgung bis hin zu Bußgeldforderungen.
7.	**Ist den Mitarbeitenden die Meldekette im Falle eines IT-Sicherheitsvorfalles bekannt?**	☐	☐	▪ Definieren Sie, an wen sich Mitarbeitende intern bei Sicherheitsvorfällen wenden können und sollen. ▪ Dies schließt auch mögliche externe Meldepflichten gegenüber Behörden oder dem Datenschutzbeauftragten ein. ▪ Der Notfallplan muss allen Mitarbeitenden bekannt sein.
8.	**Gibt es einen standardisierten und umgesetzten Onboarding-Prozess?**	☐	☐	Verschriftlichen Sie den Onboarding-Prozess und erstellen Sie eine Checkliste (Erledigungen am ersten Tag, Erstschulungen, Ausgabe Useraccount und Hardware, Schlüsselausgabe etc.).

Mitarbeitende: Schwachstellen-analyse und Maßnahmen

IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
9. Gibt es einen standardisierten und umgesetzten Offboarding-Prozess?	☐	☐	▪ Verschriftlichen Sie den Offboarding-Prozess und erstellen Sie eine Checkliste. Diese regelt bspw. IT-Rückgabeformulare, rechtzeitige Deaktivierung oder Löschung von Berechtigungen, Rückgabe von Zutrittskarten und Schlüsseln und die Datenlöschungen nach Ablauf von Aufbewahrungsfristen. ▪ Involvieren Sie dazu alle relevanten Abteilungen oder Personen.
10. Ist vertraglich geregelt, dass vereinbarte Schweigepflichten, auch hinsichtlich betrieblicher Interna (z. B. Technikgestaltung) auch nach Austritt fortgelten?	☐	☐	Prüfen und ergänzen Sie ggf. Ihre Geheimhaltungsverpflichtung, Arbeitsverträge oder Muster von Kündigungsschreiben.

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** oder rufen Sie uns unter der **Cyberhotline 030 166 360 580** an.