FAKTENBLATT

Checkliste für die Datensicherheit bei der Einarbeitung neuer Mitarbeiter

Haben Sie kürzlich neue Mitarbeiter in Ihrem Unternehmen begrüßt? Wenn dies der Fall ist, ist es von entscheidender Bedeutung, die Informationssicherheit von Beginn ihrer Beschäftigung an zu berücksichtigen. Fehler oder Unachtsamkeiten von Mitarbeitern sind eine der Hauptursachen für Datenschutzverletzungen, und eine gründliche Einweisung kann das Risiko erheblich mindern. Manager und Führungsteams können dazu beitragen, eine umfassende Sicherheitskultur in einem Unternehmen aufzubauen und zu stärken, indem sie Strategien aufzeigen und sicherstellen, dass die Mitarbeiter ihre Rolle bei der Datensicherheit erkennen.

WUSSTEN SIE DAS?

Fast die Hälfte (49 %) der befragten Unternehmensleiter gibt an, dass das mangelnde Verständnis der Bedrohungen und Risiken für das Unternehmen das größte Hindernis für die Befolgung von Informationssicherheitsrichtlinien durch die Mitarbeiter darstellt.1

Im Folgenden finden Sie eine Checkliste mit Themen zur Informationssicherheit, sowohl in elektronischer als auch in Papierform, die Sie während der Einarbeitung überprüfen sollten.

☐ **Meldung von Vorfällen.**
Trotz der besten Bemühungen eines Unternehmens kann es zu einer Datenschutzverletzung kommen. Die Mitarbeiter sollten wissen, wann und wie sie diese Vorfälle melden können, und sie sollten sicher sein, dass sie nicht bestraft werden, wenn sie sich zu Wort melden. Stellen Sie sicher, dass Sie Ihre neuen Mitarbeiter von Anfang an über die Wahrnehmungen und Erwartungen in Bezug auf die Meldung von Vorfällen informieren, damit sowohl neue als auch bestehende Mitarbeiter wissen, wie sie im Falle einer Datenschutzverletzung zu reagieren haben.

☐ **Vorschriften zur Informationssicherheit.**
Datenschutzverletzungen können zu Geldstrafen führen und den Ruf eines Unternehmens schädigen. Wenn sich die Mitarbeiter mit den wichtigsten Aspekten der einschlägigen Datensicherheitsgesetze vertraut machen, können sie einen wertvollen Beitrag zu wichtigen Diskussionen über die Datensicherheit leisten.

☐ **Druckverfahren.**
Häufige Fehler, wie das versehentliche Ablegen vertraulicher Dokumente an Orten wie Druckern, erhöhen das Risiko von Datenschutzverletzungen. Es ist wichtig, darauf hinzuweisen, wie wichtig es ist, gedruckte Materialien schnell aus dem Drucker zu holen, da dies die Wahrscheinlichkeit des Diebstahls von Informationen verringern kann. Wenn Ihr Unternehmen seine Drucker mit Passwörtern schützt, vergessen Sie nicht, neue Mitarbeiter darin zu schulen, wie sie auf diese Passwörter zugreifen und sie schützen können.

☐ **Richtlinien für elektronische Geräte.**
Persönliche Mobiltelefone und Tablets am Arbeitsplatz sind praktisch, können aber ein erhöhtes Risiko für Sicherheitsvorfälle darstellen. Stellen Sie bei der Einarbeitung neuer Mitarbeiter sicher, dass diese wissen, wie sie ihre Geräte jederzeit schützen können.

Quelle: 1 Shred-it Datenschutzbericht, 2021

Wir schützen das, was wirklich zählt.

Shred-it®
Ein Unternehmen von Stericycle®

CHECKLISTE FÜR DIE DATENSICHERHEIT BEI DER EINARBEITUNG NEUER MITARBEITER

☐ **Einen aufgeräumten Schreibtisch zu haben.**
Wenn Ihr Unternehmen eine offizielle Clean-Desk-Richtlinie hat, sollten Sie genau erklären, was das für neue Mitarbeiter bedeutet. In der Regel bedeutet dies, dass die Mitarbeiter alle Papiere mit vertraulichen Informationen unter Verschluss halten, nicht benötigte Dokumente von der Schreibtischoberfläche entfernen und die Bildschirmsperre des Computers aktivieren, bevor sie den Arbeitsplatz für längere Zeit oder am Ende des Tages verlassen.

Klicken Sie hier für eine Clean Desk Policy.

☐ **Passwort-Protokolle.**
Passwörter sind eine wichtige Sicherheitsvorkehrung. Neue Mitarbeiter sollten umfassend über die Passwortpolitik Ihres Unternehmens informiert werden und wissen, was es bedeutet, sichere Passwörter zu erstellen. Ein gutes Passwort besteht aus Groß- und Kleinbuchstaben, Zahlen und Symbolen und muss regelmäßig aktualisiert werden. Wenn in Ihrem Unternehmen ein Programm zur Aktualisierung von Passwörtern vorgeschrieben ist, sollten Sie sicherstellen, dass neue Mitarbeiter darüber informiert sind.

☐ **Umfassende Dokumentenentsorgung.**
Neue Mitarbeiter müssen genau wissen, wie sie die Dokumente Ihres Unternehmens ordnungsgemäß entsorgen können. Die Unterrichtung neuer Mitarbeiter über die bestehenden Verfahren zur Entsorgung von Dokumenten kann dazu beitragen, die Risiken zu mindern und Komplikationen beim Datenschutz zu vermeiden. Möglicherweise ist es am besten, eine "Shred-it-All"-Politik einzuführen und sie anzuweisen, alle Dokumente in einer sicheren Konsole zu entsorgen, um eine sichere Vernichtung zu gewährleisten. Auf diese Weise wird das Rätselraten darüber, was vertraulich sein könnte und was nicht, ein Ende haben. Dies trägt nicht nur zur Sicherheit vertraulicher Dokumente bei, sondern ist auch im Hinblick auf die Nachhaltigkeit von Vorteil, da das gesamte geschredderte Papier recycelt wird.

Klicken Sie hier für eine Shred-it All Policy.

☐ **Vorsichtsmaßnahmen per E-Mail.**
Vorfälle im Bereich der Cybersicherheit entstehen oft dadurch, dass Mitarbeiter auf E-Mails klicken, die sie nicht lesen sollten. Neue Mitarbeiter sollten darin geschult werden, wie sie verdächtige E-Mails, einschließlich Malware, Phishing-Programme und Ransomware, erkennen können, damit sie lernen, schädliche Situationen zu vermeiden.

Weitere Informationen über bewährte Praktiken für die Informationssicherheit finden Sie unter shredit.de oder unter der Nummer 0800 0281160

Wir schützen das, was wirklich zählt.

Shred-it®
Ein Unternehmen von Stericycle®