value one

Developing spaces, delivering smiles.

Allgemeine IT-Richtlinie der Value One Gruppe

In unserer digitalen Arbeitswelt sind Daten- und IT-Sicherheit unerlässlich. Unsere Mitarbeiter:innen arbeiten täglich mit einer Vielzahl von Daten, von Kund:innendetails bis hin zu vertraulichen Unternehmensinformationen. Es ist unsere Priorität, diese Daten bestmöglich zu schützen, um Datenspionage und Datenverluste zu verhindern.

1. Clean Desk und Passwörter

An unserem Headquarter leben wir das Prinzip des "Clean Desk". Das bedeutet, dass wir alle Mitarbeitende dazu ermutigen, ihren Arbeitsplatz sauber zu halten und sensible Unterlagen sicher zu verstauen, wenn sie ihren Arbeitsplatz verlassen. Das ermöglicht nicht nur ein flexibles Arbeiten, sondern schützt auch sensible Informationen vor unbefugtem Zugriff. Computer müssen immer gesperrt werden, wenn der Arbeitsplatz verlassen wird.

Passwörter sind für uns ein entscheidender Schutzmechanismus vor unbefugtem Zugriff. Wir fordern unsere Mitarbeiter;innen auf, einzigartige Passwörter für verschiedene Zugänge zu verwenden und diese regelmäßig zu ändern. Passwörter sollten eine Kombination aus verschiedenen Zeichen enthalten und niemals an Dritte weitergegeben werden. Bei Verdacht auf eine Kompromittierung des Passworts sollte dieses sofort geändert werden.

2. Datenspeicherung und -entsorgung

Wir legen großen Wert auf die sichere Speicherung und Entsorgung von Daten. Alle Daten müssen in den dafür vorgesehenen Bereichen, wie Netzlaufwerken oder speziellen Dokumentenmanagementsystemen, gespeichert werden. Die Verwendung lokaler Speichermedien wie Festplatten oder USB-Sticks ist nicht zulässig.

Bei der Entsorgung von Datenträgern ist größte Sorgfalt geboten. Datenträger wie USB-Sticks, Festplatten, SD-Karten und CDs/DVDs dürfen nicht einfach weggeworfen werden, sondern müssen sicher entsorgt werden.

Auch bei der Entsorgung von Dokumenten ist Vorsicht geboten. Dokumente, die sensible Daten enthalten, dürfen nicht einfach weggeworfen werden, sondern müssen sicher entsorgt werden (z.B. geschreddert werden). Sensible Daten umfassen alle personenbezogenen Daten und Informationen, deren Weitergabe oder Veröffentlichung dem Unternehmen schaden könnte.

3. Nutzung von Internet und E-Mails

In der Value One Gruppe legen wir großen Wert auf die sichere und verantwortungsbewusste Nutzung des Internets und von E-Mails. Wir fordern alle unsere Mitarbeiter:innen auf, beim Surfen im Internet äußerste Vorsicht walten zu lassen und die Weitergabe persönlicher Daten auf sichere Verbindungen zu beschränken.

E-Mails sind oft ein Einfallstor für Schadsoftware. Mitarbeiter:innen sollen keine Anhänge von unbekannten oder verdächtigen Absendern öffnen und keine Links in E-Mails anklicken, deren Quelle nicht vertrauenswürdig ist. Phishing-Mails, die zur Übermittlung von persönlichen Daten auffordern, sind sofort zu löschen.

Bei jeglichen Unsicherheiten steht unsere IT-Abteilung zur Verfügung und bietet Unterstützung. Mitarbeiter:innen sollen außerdem, vor einer Abwesenheit, den Abwesenheitsassistenten aktivieren, um Absender über ihre Nichtverfügbarkeit zu informieren.

4. Social Hacking

In der Value One Gruppe sind wir uns der Bedrohung durch Social Hacking bewusst. Dieses Phänomen bezeichnet den Versuch, durch Manipulation von Personen unbefugten Zugang zu vertraulichen Informationen oder IT-Systemen zu erlangen. Oft geben sich die Angreifer als Mitarbeiter:innen oder Vertreter:innen vertrauenswürdiger Organisationen aus.

Social Hacking ist häufig erfolgreicher als herkömmliche Hacking-Methoden. Daher fordern wir unsere Mitarbeiter:innen auf, bei ungewöhnlichen Anfragen per Telefon oder E-Mail äußerste Vorsicht walten zu lassen. Vertrauliche Informationen dürfen niemals ohne vorherige Überprüfung weitergegeben werden. Bei finanziellen Transaktionen ist stets das Vieraugenprinzip anzuwenden.

Alle verdächtigen Aktivitäten, Warnungen oder Fehlermeldungen sind unverzüglich an die IT-Abteilung zu melden.