ViCoTec
IT-SICHERHEIT & DATENSCHUTZ

Datenschutz-Checkliste für Mitarbeiter in mobiler Arbeit

Meetings, Mails, Projektsprints, dazu auch noch Datenschutz. Wir wissen, dass die Arbeitswelt stetig im Wandel ist und täglich mit neuen Herausforderungen auf Sie wartet. Damit Ihr Kopf für die wirklich wichtigen Dinge frei ist, haben wir Ihnen hier einen kleinen Leitfaden zur Verfügung gestellt, mit dem für Sie Datenschutz in mobiler Arbeit keine Hürde mehr darstellt.

Gestaltung des Heimarbeitsplatzes

- ☐ Schließen Sie Mithörende von wichtigen Telefonaten aus, z. B. durch das Schließen der Tür.
- ☐ Wichtige Dokumente müssen vor dem Einblick von Familie und Freunden geschützt werden.
- ☐ Der Bildschirm ist auch vor dem Einblick Fremder, z. B. durch folierte Fenster, zu schützen.
- ☐ Am Ende des Tages müssen alle vertraulichen Materialien sicher vor dem Zugriff Dritter geschützt sein, z. B. durch einen abschließbaren Container.
- ☐ Aktivieren Sie beim Verlassen des Arbeitsplatzes immer die Desktopsperre.
- ☐ Smart-Home Geräte wie z. B. Alexa müssen sich außerhalb des Arbeitsraumes befinden.

Genutzte Hardware

- ☐ Es werden ausschließlich vom Betrieb gestellte und administrierte Laptops für dienstliche Zwecke verwendet.
- ☐ Gleiches gilt möglichst auch für Smartphones und Tablets.
- ☐ Für dienstliche Ausdrucke sollte der vom Arbeitgeber gestellte Drucker verwendet werden.

Der richtige Umgang mit Papierdokumenten

- ☐ Für den Transport von vertraulichen Dokumenten müssen Mappen mit geeignetem Sicherheitsniveau genutzt werden z. B. verschließbare Dokumentenmappen.
- ☐ Beim Mitführen vertraulicher Dokumente muss der direkte Heimweg gewählt werden.
- ☐ Verwenden Sie keine originalen Dokumente.
- ☐ Dokumente müssen im Homeoffice datenschutzkonform, entsprechend den betrieblichen Richtlinien, vernichtet werden.

ViCoTec
IT-SICHERHEIT & DATENSCHUTZ

Virtuelle Meetings

- ☐ Die Videokonferenz muss durch ein starkes Passwort abgesichert werden.
- ☐ Der Hintergrund sollte während einer Videokonferenz unscharf gestellt werden.
- ☐ Es muss sichergestellt sein, dass vertrauliche Gespräche nicht versehentlich durch Unbefugte mitgehört werden.

Eine sichere Verbindung herstellen

- ☐ Bei Nutzung des Arbeitslaptops muss zu Beginn die VPN-Verbindung aktiviert sein.
- ☐ Das hauseigene WLAN muss nach dem aktuellen Stand der Technik verschlüsselt sein, z. B. WPA2
- ☐ Achten sie darauf, dass die automatischen System-Updates für dienstliche Geräte aktiviert sind.

Hand in Hand mit der Cloud

- ☐ Zum Verbinden mit der Cloud muss ein starkes Passwort genutzt werden.
- ☐ Werden Möglichkeiten zur sicheren Anmeldung angeboten, wie z. B. die 2-Faktor-Authentifizierung, müssen diese genutzt werden.

Mit den Kollegen in Verbindung bleiben

- ☐ Dienstliche E-Mails dürfen nicht an private Postfächer geschickt werden.
- ☐ Nutzen Sie zur dienstlichen Kommunikation nur die im Unternehmen vorgesehen Kommunikationskanäle.
- ☐ Es sollte die vom Arbeitgeber zur Verfügung gestellte Telefonanlage für dienstliche Zwecke genutzt werden.