Muster: Richtlinie für mobiles Arbeiten

Durch die Freiheiten des in unserem Unternehmen üblichen mobilen Arbeitens ergeben sich zwangsläufig auch Gefahren für die Datensicherheit. Um diese Gefahren minimal zu halten, beachten Sie bitte die folgende Richtlinie zum mobilen Arbeiten.

1. Technische Sicherung der Endgeräte

- Verschlüsselung: Mobile Endgeräte und mobile Datenträger (Laptops, USB-Sticks) müssen über eine aktivierte Festplattenverschlüsselung verfügen (z. B. BitLocker für Windows, FileVault für macOS), die zentral überwacht wird.
- Zugriffsschutz: Endgeräte werden technisch erzwungen durch Passcode und Zwei-Faktor-Authentifizierung (2FA) geschützt.
- Automatische Sperre: Der Bildschirm sperrt sich automatisch nach fünf Minuten Inaktivität. Diese Einstellungen sind zentral vorgegeben.
- Virenschutz: Alle Geräte verfügen über eine zentral verwaltete Virenschutzsoftware (Endpoint Protection).

2. Netzwerknutzung und Internet

- VPN-Pflicht: Der Zugriff auf Unternehmensressourcen erfolgt ausschließlich über eine VPN-Verbindung. Ohne VPN dürfen keine Unternehmensdaten verarbeitet werden.
- WLAN-Sicherheit: Das Benutzen öffentlicher oder unsicherer WLANs mit Firmenhardware ist untersagt.
- Webseiten-Verschlüsselung: Die Nutzung unverschlüsselter Webseiten (http statt https) ist untersagt; der Browser erzwingt verschlüsselte Verbindungen.

3. Umgang mit Daten, Datenträgern und KI

- Gerätetrennung: Das Überspielen von firmeneigenen Dateien auf private Endgeräte ist untersagt.
- Fremd-Hardware: Das Verbinden von nicht-firmeneigenen Datenträgern (USB-Sticks, externe Festplatten etc.) mit Firmenhardware ist untersagt.
- KI-Tools: Die Nutzung von nicht ausdrücklich durch das Unternehmen genehmigten KI-Tools (z. B. ChatGPT, DeepL, Midjourney) für geschäftliche Zwecke oder zur Verarbeitung von Unternehmensdaten ist untersagt.
- Datentrennung: Die Speicherung und Lagerung von privaten und geschäftlichen Daten erfolgen grundsätzlich getrennt voneinander. Getrennt bedeutet: separate Benutzerprofile oder Geräte, nicht nur verschiedene Ordner.

Muster: Richtlinie für mobiles Arbeiten

4. Physische Sicherheit und Arbeitsumgebung

- Sichtschutz: Verwenden Sie bei der öffentlichen Nutzung (Bahn, Café, Flugzeug etc.) Sichtschutzfolien.
- Virtuelle Hintergründe: Bei Videokonferenzen ist die Nutzung von Weichzeichnern (Blur-Effekt) oder virtuellen Hintergründen verpflichtend, um die Einsichtnahme in die private Umgebung oder auf vertrauliche Informationen im Hintergrund zu verhindern.
- Clean-Desk-Policy: Verwahren Sie Datenträger, Unterlagen und Endgeräte stets sicher (z. B. in einem abschließbaren Schreibtisch oder Schrank). Sperren Sie den Bildschirm beim Verlassen des Raumes.
- Vertraulichkeit: Die Schweigepflicht gilt auch gegenüber Familienmitgliedern und Mitbewohnern. Diese dürfen keinen Zugriff auf Firmendokumente oder Hardware erhalten.
- Sprachassistenten: Deaktivieren Sie Geräte wie Alexa, Google Home oder Siri oder platzieren Sie diese so, dass kein Mithören möglich ist.
- Gespräche: Führen Sie vertrauliche Telefonate oder Gespräche nicht im Beisein Dritter.

5. Dokumente und Entsorgung

- Druckvorgaben: Drucken Sie nur, wenn zwingend erforderlich. Lagern Sie Ausdrucke sicher.
- Vernichtung: Entsorgen Sie Notizen, Entwürfe und Ausdrucke nicht im Hausmüll. Nutzen Sie einen geeigneten Aktenvernichter oder geben Sie Unterlagen zur Vernichtung an das Unternehmen zurück.

6. Reisen und Notfälle

- Sorgfaltspflicht: Bei Geschäftsreisen ist für ausreichende Sicherheit von Daten und Hardware zu sorgen. Die Lagerung eines Laptops im unbeaufsichtigten Auto ist untersagt.
- Meldepflicht: Der Verlust von Firmendaten/Hardware sowie Datenpannen sind unverzüglich der Geschäftsleitung zu melden.
- Sensibilisierung: Es werden regelmäßige Schulungen durch unseren Datenschutzbeauftragten durchgeführt.