

USB, Geräte und mobile Arbeit

- [7.1 Unbekannte USB-Sticks](#)
- [7.2 Private Geräte](#)
- [7.3 Notebook unterwegs](#)
- [7.4 Öffentliches WLAN](#)
- [7.5 VPN](#)

7.1 Unbekannte USB-Sticks

USB-Sticks können Dateien und in bestimmten Fällen auch schädliche Inhalte enthalten. Ein gefundener oder unbekannter Datenträger sollte deshalb nicht aus Neugier an einen Firmencomputer angeschlossen werden.

Vergleich aus dem Alltag

Ein gefundener Schlüssel wird auch nicht nacheinander in alle Türen gesteckt, um herauszufinden, wo er passt.

Beispiel aus dem Arbeitsalltag

Auf dem Parkplatz liegt ein USB-Stick mit der Aufschrift „Löhne 2026“.

Was soll ich tun?

Neugier ist kein Grund, unbekannte Datenträger anzuschließen.

bekannte Datenträger sind nicht automatisch vertrauenswürdig



“ **Merke:** Nicht anschließen. An die zuständige Stelle oder IT geben.

7.2 Private Geräte

Private Geräte und Firmen-IT haben unterschiedliche Sicherheits- und Verwaltungsanforderungen. Nicht jedes private Gerät oder Zubehör sollte ohne Freigabe mit Firmensystemen verbunden werden.

Vergleich aus dem Alltag

An eine Produktionsmaschine schließt man ebenfalls nicht beliebige private Erweiterungen an.

Beispiel aus dem Arbeitsalltag

Ein privater Datenträger soll für die schnelle Übertragung geschäftlicher Dateien verwendet werden.

Was soll ich tun?

Bequem ist nicht automatisch sicher oder zulässig.

“ **Merke:** Für Datenaustausch die vorgesehenen Firmenwege verwenden und im Zweifel die IT fragen.

7.3 Notebook unterwegs

Firmen-Notebooks enthalten Zugänge und möglicherweise lokale Daten. Unterwegs müssen sie vor Verlust, Diebstahl und neugierigen Blicken geschützt werden.

Vergleich aus dem Alltag

Ein Notebook ist nicht nur ein Gegenstand, sondern kann ein Schlüssel zu weiteren Firmensystemen sein.

Beispiel aus dem Arbeitsalltag

Das Notebook bleibt sichtbar im geparkten Auto oder unbeaufsichtigt in einem öffentlichen Bereich liegen.

Was soll ich tun?

Ein verlorenes Arbeitsgerät ist ein Sicherheitsereignis und sollte schnell gemeldet werden.

“ **Merke:** Gerät möglichst bei sich behalten, Bildschirm sperren und Verlust sofort melden.

7.4 Öffentliches WLAN

Öffentliche WLANs werden von vielen unbekannten Geräten genutzt. Für geschäftliche Arbeit sollten nur vorgesehene und abgesicherte Verbindungswege verwendet werden.

Vergleich aus dem Alltag

Ein öffentliches WLAN ist wie ein Gespräch in einer Bahnhofshalle: Viele unbekannte Personen befinden sich in derselben Umgebung.

Beispiel aus dem Arbeitsalltag

Ein Notebook wird im Hotel oder Café mit einem öffentlichen Funknetz verbunden.

Was soll ich tun?

Öffentliches WLAN ist nicht automatisch gefährlich, aber auch nicht automatisch vertrauenswürdig.

“ **Merke:** Vorgesehene Sicherheitsverfahren und gegebenenfalls den Firmen-VPN verwenden.

7.5 VPN

Ein VPN baut einen verschlüsselten Verbindungstunnel zu einem vorgesehenen Firmennetz auf. Es ermöglicht den Zugriff auf dafür freigegebene interne Dienste.

Vergleich aus dem Alltag

Ein VPN ist wie ein geschützter Tunnel durch öffentliches Gelände.

Beispiel aus dem Arbeitsalltag

Außerhalb des Unternehmens wird zuerst die VPN-Verbindung aufgebaut, bevor ein interner Dienst verwendet wird.

Was soll ich tun?

VPN schützt die Verbindung, ersetzt aber keine sichere Arbeitsweise.

“ **Merke:** Nur die bereitgestellte VPN-Lösung und die vorgesehenen Zugänge verwenden.