**BYOD-Richtlinie (Bring Your Own Device)**

**1. Zweck dieser Richtlinie**

Diese Richtlinie regelt die Nutzung privater Geräte (Smartphones, Tablets, Laptops) für berufliche Zwecke. Ziel ist es, die Sicherheit von Unternehmensdaten zu gewährleisten und Verantwortlichkeiten klar festzulegen.

**2. Geltungsbereich**

Diese Richtlinie gilt für alle Mitarbeitenden, die eigene Geräte zur Ausführung beruflicher Aufgaben nutzen.

**3. Zulässige Geräte**

Erlaubt sind:

* Smartphones (Android/iOS)
* Tablets
* Notebooks/Laptops

Es dürfen nur Geräte mit aktuellem Betriebssystem verwendet werden.

**4. Sicherheitsanforderungen**

Alle privaten Geräte müssen:

* über ein sicheres Passwort oder eine Bildschirmsperre verfügen
* aktuelle Antivirensoftware installiert haben (sofern verfügbar)
* regelmäßig mit Updates versorgt werden
* bei Verlust oder Diebstahl sofort gemeldet werden
* bei Bedarf verschlüsselt werden

**5. Zugriff auf Unternehmensdaten**

Der Zugriff auf geschäftliche E-Mails, Kalender, Cloud-Dienste etc. darf nur über autorisierte Apps oder Web-Portale erfolgen.

Der Zugriff auf interne Systeme (z.B. per VPN) bedarf der vorherigen Zustimmung des IT-Verantwortlichen.

**6. Trennung von privat und geschäftlich**

Persönliche und geschäftliche Daten müssen getrennt bleiben (z.B. durch getrennte Apps oder Benutzerkonten).

Unternehmensdaten dürfen nicht auf private Cloud-Dienste übertragen werden.

Dritte (z.B. Familienangehörige) dürfen keinen Zugriff auf berufliche Daten haben.

**7. Unterstützung und Haftung**

Die IT-Unterstützung für private Geräte erfolgt nur eingeschränkt.

Mitarbeitende haften für Schäden, die durch grob fahrlässige Nutzung entstehen (z.B. fehlender Virenschutz, bewusste Umgehung von Sicherheitsvorgaben).

**8. Beendigung der Zusammenarbeit**

Beim Ausscheiden aus dem Unternehmen:

* muss der Zugriff auf alle Systeme und Daten vollständig entfernt werden
* sind ggf. geschäftliche Daten auf dem Gerät zu löschen oder an die IT zu übergeben