Praxis Name

Straße Nr.

PLZ Ort

**IT-Richtlinie**

**zum Umgang mit APPs**

**Dokumentenstatus**

|  |  |
| --- | --- |
| Organisationseinheit | Team Verwaltung |
| Klassifizierung | intern, öffentlich, geheim |
| Autor: | Autor |
| erstellt am: | Datum |
| Freigabe durch: | Freigebende/r |
| Freigegeben am: | Datum |
| Gültigkeitszeitraum | Datum1 – Datum2 |
| Überarbeitungsintervall | x Monate |
| Version: | 1.0 |
| Status: | In Bearbeitung, In Kraft, … |

**Dokumentenversionen**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Datum | Autor | Änderungen / Bemerkungen | Seiten |
| 1.0 |  |  | Initiale Version | alle |
|  |  |  |  |  |

# Einführung

Das Dokument „IT-Richtlinie – zum Umgang mit APPs“ setzt die Anforderungen der „IT-Sicherheitsrichtlinie nach § 75b SGB V und deren Anlagen zu diesem Thema um.

# Festlegungen

**Allgemeines**

Zur Erfüllung vertragszahnärztlicher Aufgaben werden in der Zahnarztpraxis Informationen elektronisch verarbeitet.

Dazu werden APPs im täglichen Praxisbetrieb genutzt.

Diese Richtlinie ist allen Mitarbeitern, die APPS nutzen, auszuhändigen.

Die Mitarbeiter sind zur Einhaltung dieser Richtlinie zu verpflichten.

**Programmerwerb**

Apps dürfen nur aus offiziellen Stores (z.B. für Apple-IOS-Geräte aus dem „App Store“ oder Android-Geräte aus dem „Google Play Store“) heruntergeladen werden.

**Lizenzen**

Es darf nur lizenzierte Software installiert werden.

Hierzu erfolgt eine zentrale Anforderung, Genehmigung und Beschaffung von Software/Apps.

**Umgang mit Updates**

Die App-Versionen müssen durch regelmäßige Updates auf dem aktuellen Stand gehalten werden.

Die Updates sind zeitnah durch Administratoren einzuspielen.

**Datenspeicherung**

Die Datenspeicherung von Daten und Informationen darf nur lokal erfolgen.

Es dürfen keine Daten in der Cloud abgelegt werden (Datenschutz).

Die Datensicherungen (Backups) sind auf einem firmeneigenen Datenspeicher in verschlüsselter Form abzulegen.

**Datenschutzeinstellung**

Datenschutzeinstellungen sind von den Administratoren vorzunehmen.

Es sind restriktive Einstellungen zu wählen, um persönliche Daten optimal zu schützen

Insbesondere Programmzugriffe auf Kameras, Mikrofon, Adressbücher, Kontaktdaten und Bilder sind stark einzuschränken.

Kommerzielle Messenger-Systeme sind für die Nutzung auf dienstlichen Geräten nicht zugelassen.

# Inkrafttreten

Diese Richtlinie tritt mit der Unterzeichnung in Kraft.

Ort, den

………………………………………….

Praxisinhaber