Praxis Name

Straße Nr.

PLZ Ort

**IT-Richtlinie**

**für mobile Geräte**

**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 – für mobile Geräte“ setzt die Anforderungen der „IT-Sicherheitsrichtlinie nach § 75b SGB V und deren Anlagen zu diesem Thema um.

# Festlegungen

**Allgemeines – mobile Geräte**

Die Informationsverarbeitung spielt eine wichtige Rolle bei der Erfüllung der vertragszahnärztlichen Aufgaben. Dazu werden mobile Geräte wie Smartphones und Tablets und Mobiltelefone eingesetzt.

Die mobilen Geräte werden von der Praxis für berufliche Zwecke bereitgestellt. Für private Zwecke dürfen die mobilen Geräte nicht verwendet werden.

Diese Richtlinie ist allen Mitarbeitern, die ein mobiles Gerät erhalten bzw. benutzen, auszuhändigen. Die Mitarbeiter sind zur Einhaltung dieser Richtlinie zu verpflichten.

**Mobile Device Management (MDM)**

Nur benannte Administratoren dürfen das MDM bedienen, und damit die mobilen Geräte über das MDM verwalten. Den Endnutzern ist eine eigenständige Administration der mobilen Geräte versagt.

Die Verbindung zwischen den mobilen Geräten und dem MDM wird mittels Zertifikaten geschützt. Die Verwaltung der Zertifikate erfolgt über das MDM.

Das MDM unterstützt die Fernlöschung der Daten auf den mobilen Geräten (z.B. nach Verlustmeldung).

Das MDM unterstützt das Verwalten (Installieren, Update, Löschen) von Anwendungen auf den mobilen Geräten. Dadurch werden nur aktiv zugelassene Anwendungen auf den mobilen Geräten verwendet.

Das MDM unterstützt das Verwalten (Aktivieren, Konfigurieren, Deaktivieren) von Diensten und Hardwarefunktionalitäten auf den mobilen Geräten. Dadurch werden nur aktiv zugelassene Dienste und Hardwarefunktionalitäten auf den mobilen Geräten verwendet.

Das MDM unterstützt das Verwalten von Gruppen und Profilen, um den verschiedenen Benutzern verschiedene Berechtigungen – je nach Rolle – auf den mobilen Geräten zu gewähren.

**Beschaffung**

Die mobilen Geräte werden (nach Bedarfsmeldung und Genehmigung) zentral beschafft.

**Erstkonfiguration**

Die mobilen Geräte sind vor der Ausgabe zu härten, d.h. alle verfügbaren (Sicherheits-) Updates sind einzuspielen. Alle zugelassenen Anwendungen sind in einer White-List vertreten. Alle anderen Anwendungen und Schnittstellen sind zu löschen bzw. zu deaktivieren.

Die SIM-Karte ist durch eine PIN zu schützen.

Ein komplexer Gerätesperrcode wird eingerichtet.

Der Speicher der mobilen Geräte wird verschlüsselt.

**Zugriffsschutz**

SIM-Karten sind mit einer PIN zu schützen. Die PIN ist für Notfälle in der Praxis an zentraler Stelle hinterlegt.

Die Benutzung des Gerätes ist der Startbildschirm mit einem Zugriffsschutz (Zahlencode/Streichmuster/…) vor unberechtigtem Zugriff zu schützen. Der Zugriffsschutz darf nicht deaktiviert werden und muss eine Mindestlänge von 6 Zeichen umfassen.

Die Bildschirmsperre ist zu aktivieren und auf wenige Minuten voreinzustellen.

Bei 5-facher Falscheingabe des Zugriffscodes erfolgt eine Sperrung des Gerätes.

Entsperrt werden kann das Gerät danach nur durch einen Administrator.

Ablageort (Ort benennen)

Bildschirmsperre (Anzahl) Minuten

**Sprachassistenten**

Sprachassistenten dürfen auf mobilen Geräten nicht verwendet werden.

**Geräteadministration**

Die Administration der mobilen Geräte erfolgt zentral. Dies umfasst das Installieren neuer Anwendungen (aus sicheren Quellen) und das Aktualisieren der Anwendungen und Betriebssysteme. Neue Anwendungen bzw. verfügbare Aktualisierungen für bestehende Anwendungen und Betriebssysteme sollten vor dem Installieren in einer sicheren Umgebung auf unerwünschte Effekte (Kompatibilitätsprobleme, Sicherheitslücken, etc.) getestet werden.

Die Mitarbeiter dürfen keine Anwendungen und Apps eigenständig installieren.

**Erlaubte Datenübertragung**

Mittels Mobiltelefonen dürfen folgende Daten übertragen werden:

Die Daten sind auf dem Transportweg mindestens per TLS zu verschlüsseln.

|  |  |
| --- | --- |
| Daten | Zweck |
|  |  |
|  |  |

**Geräteentsorgung**

Die mobilen Geräte werden zentral entsorgt. Dienstliche und personenbezogen Daten sind vorher sicher zu löschen.

**Geräteverlust**

Der Verlust mobiler Geräte ist unverzüglich zu melden.

SIM-Karten sind nach der Verlustmeldung zu sperren.

Dienstliche und personenbezogen Daten sind aus der Ferne zu löschen.

**Ausschlüsse**

Es ist ausgeschlossen erhöhte Berechtigungen auf den mobilen Geräten zu erhalten (z.B. durch „rooten“ bei Android oder „jailbreak“ bei IOS).

# Inkrafttreten

Diese Richtlinie tritt mit der Unterzeichnung in Kraft.

Ort, den

………………………………………….

Praxisinhaber