Praxis im Tiergartentower

RICHTLINIE - für Mitarbeiter zur Benutzung von mobilen Geräten

PiTt_RL_MG

[Organisationseinheit]

[Autor]

[Datum]

[Version]

INHALT

DOKUMENTENLENKUNG

Dokumententyp:	Richtlinie
Klassifizierung	[intern, öffentlich, geheim]
Editor:	[Editor]
Editiert am:	[Datum]
Prüfer:	[Prüfer]
Geprüft am:	[Datum]
Freigeber:	[Freigeber]
Freigegeben am:	[Datum]
Gültigkeitszeit	[]
Überarbeitungsintervall	[]
Version:	1.0
Status:	[In Bearbeitung, In Kraft, …]

DOKUMENTENSTATUS

Version	Datum	Autor	Änderung	Begründung	Seite
1.0	[Datum]	[Autor]		Initiale Version	alle

0. Vorwort

Dieses Dokument „Richtlinie - für Mitarbeiter zur Benutzung von mobilen Geräten“ ist ein Musterdokument einer fiktiven Arztpraxis „Praxis im Tiergartentower“. Es dient zur Vorlage um die Anforderungen der „Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“ und deren Anlagen umzusetzen.
Das Dokument steht zur freien Verfügung. Falls das Dokument als Vorlage für eine eigene Richtlinie verwendet wird, empfiehlt es sich mindestens die gelb Hinterlegten Textpassagen entsprechend anzupassen.

1. REGELUNGEN

1.1 Mobile Geräte

Die PiTt ist eine niedergelassene Vertragsarztpraxis.

Die Informationsverarbeitung spielt eine Schlüsselrolle für die Erfüllung dieser Aufgaben. Dabei werden auch 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, auszuhändigen. Die Mitarbeiter sind zur Einhaltung dieser Richtlinie zu verpflichten.

1.2 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 damit versagt.

Die Verbindung zum der mobilen Geräte zum 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 Hardware-Funktionalitäten auf den mobilen Geräten. Dadurch werden nur aktiv zugelassene Dienste und Hardware-Funktionalitäten 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.

1.3 Beschaffung

Die mobilen Geräte werden [nach Bedarfsmeldung und Genehmigung] zentral beschafft.

1.4 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 ein PIN zu schützen.

Ein komplexer Gerätesperrcode wird eingerichtet.

Der Speicher die mobilen Geräte wird verschlüsselt.

1.5 Sprachassistenten

Sprachassistenten dürfen auf mobilen Geräten nicht verwendet werden.

1.6 Administration

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 ungewünschte Effekte (Kompatibilitätsprobleme, Sicherheitslücken, etc.) getestet werden.

Die Mitarbeiter dürfen keine Anwendungen und Apps eigenständig installieren.

1.7 Erlaubte Datenübertragung

Mittels Mobiltelefonen dürfen folgende Daten übertragen werden:

Die Daten sind dabei mindestens auf den Transportweg per TLS zu verschlüsseln.

Daten	Zweck

1.8 Entsorgung

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

1.9 Verlustmeldung

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.

1.10 Verbote

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

2. INKRAFTSETZUNG

Berlin, den [Datum]

[Inhaber]