

## Checkliste zur IT-Sicherheitsrichtlinie für Arztpraxen

Diese Checkliste basiert auf den Vorgaben der Kassenärztlichen Bundesvereinigung (KBV) und unterstützt Arztpraxen bei der Umsetzung der IT-Sicherheitsrichtlinie.

### 1. Technische Schutzmaßnahmen

- Firewall vorhanden und korrekt konfiguriert
- Aktuelle Antivirensoftware installiert
- Regelmäßige Software-Updates
- Automatisierte Datensicherung mit Wiederherstellungstest
- Segmentierung und Schutz des Netzwerks

### 2. Organisatorische Maßnahmen

- Zugriffsrechte nach Minimalprinzip vergeben
- Starke Passwortregeln implementiert
- Regelmäßige Mitarbeiterschulungen zur IT-Sicherheit
- Onboarding/Offboarding-Prozesse für IT-Zugänge vorhanden

### 3. Dokumentation und Prozesse

- Schriftliche IT-Sicherheitsrichtlinie vorhanden
- Aktueller Netzplan der IT-Infrastruktur
- Dokumentierte Verfahren zu IT-Prozessen
- Prozess für IT-Sicherheitsvorfälle definiert

### 4. Nutzung von Cloud-Diensten

- Zertifizierte Cloud-Anbieter (z. B. C5-Testat) gewählt
- Auftragsverarbeitungsverträge mit Anbietern vorhanden
- Datenübertragung und -speicherung verschlüsselt

### 5. Mobile Geräte und Telematikinfrastruktur

- Zentrales Mobile Device Management (MDM) vorhanden
- Regelung zur privaten Gerätenutzung definiert
- Sichere TI-Installation (Konnektor, Kartenterminals, etc.)

Weitere Informationen und Musterdokumente zur Umsetzung:

<https://www.kbv.de/html/it-sicherheit.php>

<http://www.kbv.de/praxischeck>

## Anhang: Anforderungen der KBV an alle Praxen (Stand: 2025)

- ✓ Schulung des Praxispersonals im sicheren Umgang mit IT – Anlage 1 Nr. 9
- ✓ Regelmäßige Schulungen zur eingesetzten Technik – Anlage 1 Nr. 6
- ✓ Schulungen nach Aufgabenverantwortung – Anlage 1 Nr. 10
- ✓ IT-Einarbeitung neuer Mitarbeiter – Anlage 1 Nr. 1
- ✓ Passwortänderung bei Personalwechsel – Anlage 1 Nr. 2
- ✓ Verpflichtung & Aufsicht bei IT-Dienstleistern – Anlage 1 Nr. 3
- ✓ Regelung zum Umgang mit Spam – Anlage 1 Nr. 41
- ✓ Aktuelle Virenschutzprogramme – Anlage 1 Nr. 20
- ✓ Apps nur aus offiziellen Stores – Anlage 1 Nr. 42
- ✓ Keine vertraulichen Daten per App – Anlage 1 Nr. 44
- ✓ Gerätesperrcode bei mobilen Geräten – Anlage 1 Nr. 32
- ✓ Abmeldung nach Nutzung – Anlage 1 Nr. 19
- ✓ Netzplan vorhanden – Anlage 1 Nr. 12
- ✓ Web Application Firewall bei Online-Angeboten – Anlage 1 Nr. 47
- ✓ Keine automatisierten Webzugriffe – Anlage 1 Nr. 48
- ✓ Planmäßige Datensicherung – Anlage 1 Nr. 21
- ✓ SIM-Sperre bei Geräteverlust – Anlage 1 Nr. 34
- ✓ Wechseldatenträgerprüfung auf Schadsoftware – Anlage 1 Nr. 36
- ✓ Nur verschlüsselte Apps zur Dokumentenspeicherung – Anlage 1 Nr. 43
- ✓ Updates für TI-Komponenten – Anlage 5 Nr. 8
- ✓ Sichere Aufbewahrung von TI-Administrationsdaten – Anlage 5 Nr. 9