SECUREPOINT

KBV-RICHTLINIEN ERFÜLLEN

Patientendaten schützen

Wir schützen Ihre Daten und die Ihrer Patienten mit der Vielfalt von Unified Security.

Sichere KIM

Schützt Kanäle zur Kommunikation im Medizinwesen vor Viren, Phishing, Spy- und Malware.

Mobil- und Großgeräte sichern

Mit Unified-Security-Lösungen alle webfähigen Endgeräte zuverlässig schützen.

Verschiedene Bereiche

Schutz für alle Arten von Praxen, Laboren medizinischen Versorgungszentren und mehr.

SICHERE NETZWERKE FÜR MEHR PATIENTENSCHUTZ

KBV-RICHTLINIEN ÜBERSETZUNG

Anforderungen gemäß KBV-Richtlinie	Erläuterung
2021	
Anlage 1/Nr. 2: Verhinderung von Datenabfluss	Vertrauen Sie beim Versand von vertraulichen Daten ausschließlich den offiziellen Kommunikationswegen wie KIM, und verzichten Sie auf Datenversand via Messenger-Apps oder privater E-Mail.
Anlage 1/Nr. 10: Kryptografische Sicherung von vertraulichen Daten	Kommunikationsweg und Ablageort müssen ausreichend verschlüsselt sein. Lösungen sind beispielsweise VPN-Verbindungen sowie passwortgeschützte, verschlüsselte Festplatten und Backups.
Anlage 1/Nr. 13: Abmelden und Sperren	Lassen Sie niemals einen PC, ein Tablet oder Smartphone im angemeldeten Zustand unbeaufsichtigt.
Anlage 1/Nr. 12: Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und -Kameras	Kameras und Mikrofone nur im konkreten Fall der Nutzung aktivieren, sonst abschalten.
2022	
Anlage 1/Nr. 3: Sichere Speicherung lokaler App-Daten	Keine Speicherung von App-Daten auf Cloud-Servern. Nur eine lokale Speicherung auf dem Gerät, und dann auch nur verschlüsselt, ist zulässig. Bei jeder Cloudspeicherung ist die Frage unklar, wer auf die dortigen Server Zugriff erhält. Ohne Verschlüsselung lassen sich lokale Daten leicht mit einem Trojaner ausspionieren.
Anlage 1/Nr. 9: Firewall benutzen	Eine Firewall kann über verschiedene Techniken den Datenstrom tiefgreifend überwachen und bei Bedarf stoppen. Gängige Router werden manchmal als Alternative dargestellt, das ist jedoch nicht richtig. Techniken wie Proxy-Server, Intrusion-Detection bzw. -prevention (also die Analyse auf laufende Angriffe und deren Abwehr) können durch Router nicht geleistet werden.
Anlage 1/Nr. 14: Regelmäßige Datensicherung	Eine Datensicherung in Form eines Backups ist absolut unverzichtbar. Gelegentliche manuelle Sicherungen auf USB-Stick oder USB-Laufwerke erfüllen die Anforderungen der KBV nicht. **Wichtig:** ▪ Speicherung automatisch ausführen (täglich) ▪ Ausschließlich Speichermedien und -orte wählen, die vor fremdem Zugriff geschützt sind ▪ Nur verschlüsselte Datensicherungen nutzen ▪ Cloud-Sicherungen nur bei europäischen Anbietern **Tipp: Führen Sie regelmäßige Wiederherstellungstests durch.**

Anforderungen gemäß KBV-Richtlinie	Erläuterung
2022	
Anlage 1/Nr. 28: Schutz vor Schadsoftware	Seien Sie extrem vorsichtig bei der Nutzung von Wechseldatenträgern (z. B. USB-Stick oder USB-Festplatten). Allein das Anschließen eines USB-Speichermedium kann die Schadsoftware übertragen! Wenn möglich, lassen Sie die Nutzung solcher Datenträger in den System-Einstellungen verbieten. Arbeitsplätze, die ohne diese Datenträger nicht sinnvoll betrieben werden können, brauchen eine immer aktuell gehaltene Schutzsoftware.
Anlage 5/Nr. 6: Zeitnahes Installieren verfügbarer Aktualisierungen	Für alle Systeme gilt: Verfügbare Updates stets so schnell wie möglich installieren! Das betrifft alle Komponenten der Telematikinfrastruktur, aber natürlich auch die Betriebssysteme der Praxisrechner und Server, alle Anwendungsprogramme inklusive Standardtools, Praxisdrucker, Kartenleser, eventuell vorhandener Kameras und anderer Netzwerkgeräte. Virtuelle Praxiscomputer oder -server und die dort installierten Systeme müssen ebenfalls berücksichtigt werden.
Anlage 5/Nr. 7: Sicheres Aufbewahren von Administrationsdaten	Alle relevanten Administrationsdaten (z. B. Anmeldenamen und Passwörter) dürfen ausschließlich berechtigten Personen zur Kenntnis gelangen. Sie sind sicher zu verwahren, also sicher vor Diebstahl, unberechtigter Einsichtnahme und vor Verlust durch Feuer oder Wasser. Das gilt für alle relevanten Daten Ihrer IT-Struktur. Es gibt Software (Passwortmanager), die dabei helfen kann. Achten Sie hierbei auf die Wahl des Anbieters.
Ab dem 1. Januar 2022	
Anlage 4/Nr. 6: Netzsegmentierung	Die Netzsegmentierung regelt den Zugriff auf bestimmte Daten und Speicherorte. Sensible Teile des Netzwerks und darin enthaltenen schützenswerten Daten werden „abgetrennt“ und der Zugriff darauf eingeschränkt. Hierdurch wird zum Beispiel verhindert, dass ein Servicetechniker am Großgerät Patientendaten einsehen kann. Ebenfalls ist so der Zugriff auf das Großgerät nur einem ausgewählten Teil der Mitarbeitenden möglich. Typischerweise wird der Zugriff über eine Firewall detailliert geregelt.

ANGEBOTE FÜR MEHR IT-SICHERHEIT IM GESUNDHEITSWESEN

Basic Pro

Für Puristen

- ✓ Black Dwarf Pro as a Service inkl. WiFi (bis 15 Arbeitsplätze)
- ✓ Infinity-Lizenz (1 Jahr)
- ✗ Kein Antivirus Pro
- ✗ Kein Mobile Security
- ✓ Inkl. Vorabaustausch-Service

Ihr Preis*

Advanced Pro

Für Sicherheitsbewusste

- ✓ Black Dwarf Pro as a Service inkl. WiFi (bis 15 Arbeitsplätze)
- ✓ Infinity-Lizenz (1 Jahr)
- ✓ 15x Antivirus Pro
- ✗ Kein Mobile Security
- ✓ Inkl. Vorabaustausch-Service

Ihr Preis*

Premium Pro

Für alle, die mehr wollen

- ✓ Black Dwarf Pro as a Service inkl. WiFi (bis 15 Arbeitsplätze)
- ✓ Infinity-Lizenz (1 Jahr)
- ✓ 15x Antivirus Pro
- ✓ 15x Mobile Security
- ✓ Inkl. Vorabaustausch-Service
- \+ Inkl. Unified Backup
- \+ Inkl. Reporting

Ihr Preis*

Änderungen und Irrtümer vorbehalten. Stand: 16.01.2023

Ich bestätige die Annahme des Angebotes:

- ☐ Basic Pro
- ☐ Advanced Pro
- ☐ Premium Pro

Die Durchführung und Installation soll über meinen Fachhandelspartner erfolgen.

Datum, Unterschrift & Stempel (Arzt-/Praxis)

*Die Mindestvertragslaufzeit (MVL) beträgt zwölf Monate. Die Mindestvertragslaufzeit verlängert sich nach deren Ablauf automatisch ohne Neubeantragung um einen weiteren Monat/weitere zwölf Monate, wenn der Vertrag nicht vier Wochen vor Ablauf der aktuellen Mindestvertragslaufzeit schriftlich gekündigt wird. Alle Preise zzgl. MwSt.

SECUREPOINT

Securepoint GmbH
Bleckeder Landstraße 28
D-21337 Lüneburg

Tel.: 0 41 31 / 24 01-0
E-Mail: info@securepoint.de
Web: www.securepoint.de

Trust Seal www.teletrust.de/itsmie

SecurITy made in EU

EU DS-GVO ready

SecurITy made in Germany

Überreicht durch Ihren Securepoint-Partner