Leistungsbeschreibung Praxis Protect S

Leistungsbeschreibung für Praxis Protect S – Endpoint Protection (Antivirenschutz)

Sehr geehrte Damen und Herren,

danke, dass Sie sich für unsere **Endpoint - Protection** entschieden haben. Mit der Endpoint Protection bieten wir Ihnen einen umfassenden Schutz für Ihren PC, der Bedrohungen wie Viren, Malware und Cyberangriffe effektiv abwehrt. Im Folgenden erhalten Sie eine detaillierte Beschreibung der enthaltenen Leistungen und Rahmenbedingungen.

1 Systemvorraussetzungen

Damit wir die Software bei Ihnen optimal einrichten können, benötigen wir einen **stabilen Breitband-Internetanschluss von mind. 5 Mbit**. Die Sicherheitslösung wird direkt auf Ihren Computern / Notebooks und Servern installiert.
Folgende Betriebssysteme werden unterstützt:

- **Windows:** ab Windows 10
- **MacOS:** ab Version 10.10

Wichtiger Hinweis: Es werden nur Betriebssysteme (Windows etc.) unterstützt die sich im Herstellersupport befinden. Durch den Hersteller abgekündigte Betriebssysteme werden nicht unterstützt.

2 Installationstermin

Zur Installation der **Endpoint Protection** wird mit Ihnen ein **Installationstermin per Fernwartung** durchgeführt. Für diesen Termin müssen Sie einen PC bereitstellen, der den beschriebenen technischen Voraussetzungen aus **Punkt 1** entspricht.

3 Zielsetzung und Umfang

Die Lösung stellt sicher, dass Ihre IT-Umgebung bestmöglich geschützt ist. Das beinhaltet:

- Schutz vor Viren, Malware und Cyberangriffen
- Regelmäßige Updates

- Einfache Integration in Ihre bestehende IT-Infrastruktur

  Bitte beachten Sie, dass Hardware nicht Bestandteil dieser Leistung ist.

4 Erweiterter Schutz

"Unsere Endpoint Protection schützt ausschließlich die Computer und Server, auf denen sie installiert ist. Sie umfasst:

4.1 Schutzmechanismen

Unsere Lösung kombiniert zwei leistungsstarke Technologien:

- **Endpoint Protection Platform (EPP):**
  - Automatische Virenscans und Schutz in Echtzeit
  - Individuelle Anpassung von Blacklists & Whitelists
  - Manipulationsschutz und E-Mail-Filterung
- **Endpoint Detection and Response (EDR):**
  - Permanente Überwachung aller Aktivitäten
  - Blockierung unbekannter Programme, bis diese als sicher eingestuft wurden
  - Automatische Bedrohungsanalyse durch künstliche Intelligenz

4.2 Vorkonfiguration & Sicherheitseinstellungen

- **Sandboxing:** Unbekannte Dateien werden in einer gesicherten Umgebung getestet.
- **Anti-Exploit-Technologie:** Schutz vor Hackerangriffen durch Schwachstellen.
- **Virenschutz:** Automatische Erkennung und Blockierung von Bedrohungen.
- **Content-Filter:** Steuerung des Internetzugriffs Ihrer Mitarbeiter.
- **Threat Hunting Service:** Proaktive Analyse verdächtiger Aktivitäten.

5 Datenschutz und Sicherheit

- DSGVO-konform: Ihre Daten bleiben geschützt.
- Keine Weitergabe an Dritte.

- Regelmäßige Sicherheitsupdates inklusive.

6 Service und Support

Unser Support-Team steht Ihnen zur Servicezeit gemäß unserer Website Allgemeine Geschäftsbedingungen (AGB) | HASOMED GmbH zur Verfügung. Sie können uns telefonisch oder per E-Mail erreichen, um Service- oder Supportanfragen zu stellen.

7 Wichtiger Hinweis

- Die Endpoint Protection bietet einen Schutz auf dem Endgerät selbst. IT-Sicherheitskomponenten können keine **100%ige Garantie gegen Cyberangriffe gewährleisten. Eine tägliche Datensicherung** gemäß den Vorgaben der **KBV IT-Sicherheitsrichtlinie** ist daher unerlässlich**.**
- Sie ersetzt keine umfassende Netzwerk-Sicherheitslösung und kann nicht das gesamte Praxis-Netzwerk absichern.
- Zusätzliche Schutzmaßnahmen, wie Firewalls oder Netzwerksicherheitslösungen, werden aus diesen Gründen ist der KBV IT-Sicherheitsrichtlinie als zwingend erforderlich aufgeführt.
- Die empfohlenen Maßnahmen entsprechen den IT-Sicherheitsrichtlinien der Kassenärztlichen Bundesvereinigung (KBV) und sollten entsprechend umgesetzt werden, um den Schutz der gesamten IT-Infrastruktur zu optimieren.