Leistungsbeschreibung - Managed Workplace

1 Leistungsumfang des Managed Workplace 1

1.1 Monitoring & Alarmierung 1

1.2 Patch-Management 1

1.3 Endpoint-Security 2

1.4 Fernwartungstools 3

1.5 Cloud-Datensicherung 3

2 Support und Service 3

3 Kündigungsfrist 4

4 Bestätigung und Dokumentation 4

1 Leistungsumfang des Managed Workplace

Die Softwarelösung *Managed Workplace* ermöglicht die Fernverwaltung und das Monitoring von Praxis – PCs. Sie übernimmt zentrale Aufgaben eines lokalen Administrators und unterstützt insbesondere psychotherapeutische Einzelpraxen dabei, ihre IT-Systeme im Einklang mit der **KBV IT-Sicherheitsrichtlinie** abzusichern und zu verwalten.

1.1 Monitoring & Alarmierung

Alle angebundenen Windows-Arbeitsplätze werden durch einen professionellen IT-Dienstleister kontinuierlich überwacht. Das Monitoring umfasst unter anderem:

- Den Zustand wichtiger Windows-Dienste
- Den Füllstand der Festplatten inklusive SMART-Analyse zur Früherkennung von Hardwarefehlern
- Den Aktualitätsstatus der Antiviren-Signaturen
- Die Auswertung kritischer Ereignisse aus den Windows-Ereignisprotokollen

Alle erkannten Warnungen, sicherheitsrelevanten Vorfälle und Systemfehler werden automatisiert analysiert und über ein integriertes Alarmierungssystem an das betreuende IT-Team weitergeleitet.

1.2 Patch-Management

Das integrierte Patch-Management gewährleistet die zuverlässige und regelmäßige Installation sicherheitsrelevanter Updates und Patches. Täglich werden Updates, die von den jeweiligen Softwareherstellern bereitgestellt und durch den IT-Dienstleister freigegeben wurden, automatisiert auf den Endgeräten installiert. Dies betrifft sowohl Microsoft-Produkte als auch gängige Drittanbieter-Software.

Zu den typischerweise unterstützten Drittanbieter-Anwendungen zählen beispielsweise:

- Microsoft Edge
- VLC Media Player
- Veeam Agent for Windows
- Mozilla Thunderbird

Diese Programmliste ist nicht abschließend und unterliegt einem kontinuierlichen Aktualisierungsprozess. Der Umfang der unterstützten Softwarepakete kann sich im Zuge technischer Entwicklungen und sicherheitsrelevanter Anforderungen dynamisch ändern.

Nicht Bestandteil des automatisierten Patch-Managements sind individuelle Fachanwendungen, wie Praxissoftware oder branchenspezifische Lösungen. Der Support für die Praxissoftware ist über das Elefant Abo abgebildet und von dem Managed Workplace differenziert zu betrachten.

(Hinweis: Eine vollständige Liste der unterstützten Softwareprodukte zum jeweiligen Zeitpunkt erhalten Sie auf Anfrage)

Die Verteilung der Updates erfolgt zentral gesteuert und automatisiert. Jeder Installationsvorgang wird systemseitig dokumentiert, um Transparenz und Nachvollziehbarkeit zu gewährleisten.

Wichtiger Hinweis:

Die HASOMED GmbH übernimmt keine Haftung für die von Softwareherstellern installierten Updates. Notwendige Reparaturen, die aufgrund fehlerhafter Updates erforderlich werden, sind vom Kunden kostenpflichtig zu beauftragen.

1.3 Endpoint-Security

Die eingesetzte Sicherheitslösung bietet umfassenden Schutz auf allen angebundenen Endgeräten durch moderne **Endpoint Protection**, unterstützt durch Technologien aus dem Bereich der künstlichen Intelligenz. Zu den enthaltenen Schutzfunktionen zählen:

- Echtzeit-Virenschutz mit automatisierter Bedrohungserkennung
- Verhaltensbasierte Analysen zur Identifikation von Malware und Anomalien
- Gerätesteuerung, z. B. USB-Zugriffsfilter
- Webfilter zur Kontrolle und Einschränkung unsicherer oder unerwünschter Webseiten
- Applikationskontrolle zur Überwachung der Nutzung installierter Programme
- Schutz vor Verschlüsselungstrojanern (Ransomware)
- Quarantänefunktionen bei identifizierten Bedrohungen
- Automatisierte Alarmierung je Endgerät bei sicherheitsrelevanten Vorfällen

1.4 Fernwartungstools

Die Managed-Workplace-Lösung beinhaltet ein vollständig integriertes Fernwartungssystem, dass eine direkte Administration der Endgeräte über eine zentrale Management-Umgebung ermöglicht.

Die eingesetzte Fernwartungstechnologie erfüllt die Vorgaben der Datenschutz-Grundverordnung (DSGVO) und wird regelmäßig sicherheits- sowie funktionsseitig aktualisiert. Dadurch wird ein effizienter, sicherer und rechtskonformer Support der angebundenen Arbeitsplätze gewährleistet.

1.5 Cloud-Datensicherung

Zur Umsetzung einer sicheren und regelkonformen Datensicherung gemäß der 3–2–1-Backup-Regel ist im Managed Workplace eine dateibasierte Cloud-Datensicherung integriert.

Diese Lösung speichert sowohl Benutzerdaten als auch in regelmäßigen Abständen ein vollständiges Systemabbild. Dadurch ist im Bedarfsfall eine schnelle Wiederherstellung des gesamten Systems möglich.

Die Datensicherung erfolgt verschlüsselt und wird anschließend in ein nach ISO/IEC 27001 zertifiziertem Rechenzentrum mit Standort in Deutschland übertragen, wodurch höchste Anforderungen an Datenschutz und IT-Sicherheit erfüllt werden.

2 Support und Service

- Im Rahmen des Managed Workplace steht dem Auftraggeber ein technischer Support zur Verfügung. Der Erstkontakt erfolgt grundsätzlich über die Elefant-Hotline (Level-1-Support) der HASOMED oder durch die Bearbeitung von Support-Tickets.
- Die Servicezeiten des Level-1-Supports entnehmen Sie bitte dem folgenden Link: https://hasomed.de/kontakt/

  Wichtiger Hinweis:
- Der Level-1-Support der HASOMED GmbH übernimmt keinen technischen Support für vom Kunden installierte Fremdsoftware auf der gelieferten IT-Hardware. Der Support beschränkt sich ausschließlich auf die in Punkt 1.1 – 1.5 beschriebenen Funktionen des Managed Workplace.

3 Kündigungsfrist

Die Vertragslaufzeit für die Dienstleistung *Managed Workplace* beträgt ab Vertragsabschluss ein Jahr. Die Kündigungsfrist beträgt drei Monate zum Ende der jeweiligen Vertragslaufzeit. Erfolgt innerhalb dieses Zeitraums keine fristgerechte Kündigung durch den Auftraggeber, verlängert sich der Vertrag automatisch um jeweils ein weiteres Jahr.

4 Bestätigung und Dokumentation

Der Auftraggeber bestätigt bei Bestellung der IT-Komponenten, diese Leistungsbeschreibung zur Kenntnis genommen, verstanden und akzeptiert zu haben. Alle relevanten Dokumente und detaillierte Herstellerinformationen werden bei Auslieferung der Komponenten zur Verfügung gestellt.