Leistungsbeschreibung ITSR Managed Service-Paket: PC - Stand: 01.05.2021

Vorbemerkung
Wenn im Folgenden das Wort Client genutzt wird, sind hiermit ebenso PCs, MACs, Workstations, Thin-Clients oder Notebooks gemeint
Wenn im Folgenden zwischen Basis, Standard und Premium unterschieden wird, gilt eine Sache für ausschließlich das/die genannte(n) Pakete, andernfalls für alle drei Pakete.
Die Mindest-Vertragslaufzeit beträgt 36 Monate. Der Vertrag verlängert sich um je zwölf Monate, sollte er nicht mit einer Frist von drei Monaten zum Ablaufdatum schriftlich gekündigt werden.
Falls bei einzelnen Leistungen Managed Service-Leistungen von Dritten genutzt werden sollten, so sichert der Auftragnehmer zu, dass diese Services in der Bundesrepublik Deutschland gehostet sind.

Voraussetzungen
Die zuverlässige, sichere und kostengünstige Betreuung innerhalb dieses Konzepts basiert auf bestimmten Voraussetzungen der IT-Struktur beim Kunden. Dies umfasst:

- Der Kunde ist für das tägliche Anfertigen einer Voll-Datensicherung sowie einer Archivierung verantwortlich, und zwar mit mindestens fünf in regelmäßigem Wechsel und an einen dritten Ort verbrachte Datenträger.
- Für die eingesetzte Hard- und Software ist erforderlich, dass sie über einen gültigen Herstellersupport (bspw. CarePack, Softwarepflegevertrag, Maintenance, Microsoft Lifecycle Support) verfügt.
- Eine Ist-Analyse mit den Komponenten der Netzwerkinfrastruktur inkl. IP-Adressliste, externe Provider-Anbindung, Firewall-Konzept, Softwarestände, Hardwareüberblick, Backup-Konzept, Ansprechpartner der involvierten Personen beim Kunden und dessen Softwarelieferanten, sowie ein Notfallplan ist vorhanden und entspricht der aktuellen Konfiguration. Sollte eine aktuelle Ist-Analyse nicht vorhanden sein, so bietet der Auftragnehmer die Umsetzung nach Aufwand gemäß Ziffer 15 an.
- Auf Basis der Erkenntnisse der Ist-Analyse ist möglicherweise die Umsetzung eines Maßnahmenplans notwendig.
- Für die Buchung der Fernwartungs-Flatrate gemäß Ziffer 16 gilt: Mindestabnahmemenge 5 Stück.

1 Web-Zugriff auf Service-Status & Meldung von Support-Servicefällen
Der Kunde erhält auf seinen Wunsch / auf Anforderung zwei Zugänge. Der erste Zugang ermöglicht die Einsichtnahme der Ergebnisse des Monitorings laut Ziffer 3 sowie den Abruf eines Monatsberichts.
Über den zweiten Zugang erhält der Kunde Zugriff auf eine Übersicht aktueller und vergangener Servicefälle. Zusätzlich ist ein Melden von neuen Problemen oder Aufgaben über dieses System möglich.

2 Fernwartungssoftware, Taskleistenapplikation
Die Fernwartungssoftware ermöglicht die zeitnahe Problemlösung durch Techniker des Auftragnehmers aus der Ferne über eine nach dem üblichen Standard gesicherte Internetverbindung. Der Auftragnehmer versichert, diesen Zugang mit hoher Sorgfalt zu verwalten und versichert weiterhin, sämtliche in Kontakt mit den Systemen des Kunden kommenden Mitarbeiter im Hinblick auf die Einhaltung der relevanten Datenschutzgesetze zu verpflichten. Die benötigten Lizenzen zur Nutzung der Fernwartungssoftware auf den Clients sind enthalten. Weiterhin stellt der Auftragnehmer dem Kunden eine über das IT-Management-System zugängliche Fernwartungs-Funktion für seine eigenen Zwecke zur Verfügung, sofern für die zu fernwartenden Geräte ein Managed Service Vertrag gebucht wurde. Bezüglich der Art des Fernwartungs-Zugriffs vereinbaren Kunde und Auftragnehmer eine Handhabung gemäß dem Dokument „Fernwartungsvereinbarung“.

3 Tägliches Monitoring
Tägliche Überwachung der Clients mit einem agentenbasierten, automatischen Software-Tool hinsichtlich der Lauffähigkeit der Windows-Dienste, Überschreitung eines Festplattenfüllstandschwellwertes, Aktualität der Anti-Virus-Signaturen, Prüfung auf kritische Ereignisse in den Windows-Ereignisprotokollen, Physischer Festplattenzustand (SMART) sofern die entsprechenden Hard- und Softwarekomponenten diese Informationen bereitstellen. Fehlermeldungen werden von technischen Mitarbeitern des Auftragnehmers interpretiert. Der Kunde erhält auf seinen Wunsch / auf Anforderung einen Zugang mit einem Nur-Lesen-Zugriff auf das IT-Management-System, um den Status seiner IT, etwaiger Fehlermeldungen und zugehöriger Maßnahmendokumentation jederzeit abrufen zu können. Für die Funktionalität wird ein Agent auf den Clients installiert, der zwingend eine ausgehende SSL-Internetverbindung (Port 443) in ein bestimmtes Zielnetz nach außen nutzt.

4 Tägliche Alarmierung durch das Monitoring
Eine Alarmierung erfolgt aus dem IT-Management-System per E-Mail an wählbare Empfänger.
Sollte es aus Sicht des Kunden notwendig sein, Fehlerlösungsmaßnahmen durch den Auftragnehmer einzuleiten, so wird der Kunde den Auftragnehmer hierzu beauftragen. Beim Standard- und Premiumpaket erfolgt die Weiterverarbeitung der Fehler direkt im Ticket-System des Auftragnehmers. Es wird in diesem Fall die Abrechnung nach Ziffer 15 vorgenommen sofern kein/e Hotline-Pakete, Stundenkontingente und/oder Flatrates vom Kunden gebucht worden sind.

5 Inventarisierung Tägliche automatische Aktualisierung der Auflistung der installierten Hard- und Softwarekomponenten der Clients im vom Auftragnehmer für den Kunden bereitgehaltenen IT-Management-System. Mit dem IT-Management-System unterstützt der Auftragnehmer die vertraglich vereinbarten Leistungen. Für die Funktionalität wird ein Agent auf den Clients installiert, der zwingend eine Internetverbindung über Port 443 nach außen nutzt. Fünf eigene Felder zur Dokumentation von Inventarnummern oder Standortdaten können hinzugefügt werden. Auswertungen bzgl. der im Einsatz befindlichen Clients sowie deren Veränderungen können jederzeit abgerufen werden. Weiterhin ist ein Export der Daten als XML-Datei möglich.

6 Wöchentlicher zusammengefasster Bericht
Der Auftragnehmer erstellt auf Wunsch / auf Anforderung des Kunden wöchentlich einen Bericht, in dem die wichtigsten Systemprüfungen der Clients zusammengefasst dargestellt sind. Dazu gehört eine Übersicht des Erfolgs konfigurierter Prüfungen wie Anti-Virus, Ereignisanzeigen und Festplattenkapazität. Der Kunde erhält den Bericht, nach seiner schriftlichen Beauftragung, per E-Mail zugesandt.

7 Softwarelizenz-Verwaltung
Beim Basis-, Standard- und Premiumpaket erfolgt die Bereitstellung eines über das Internet zugänglichen Verwaltungssystems, in dem die installierten Softwareprogramme der Clients dargestellt werden. Die Liste der lizensierten Produkte muss durch den Kunden im System hinterlegt werden. Der Auftragnehmer kann diese Leistung für den Kunden gegen Stundenverrechnung nach Ziffer 15 übernehmen, wenn der Kunde den Auftragnehmer hierzu zusätzlich beauftragen möchte. Eine tagesaktuelle Auswertung oder Erstellung eines Berichts ist jederzeit über das Verwaltungs-System möglich. Die Verantwortung für eine korrekte Lizensierung der eingesetzten Produkte liegt beim Kunden.

8 Managed Antivirus
Präambel:
Ein 100%iger Anti-Virus-Schutz ist nicht möglich. Der Auftragnehmer wird nach den üblichen Standards Maßnahmen zum Schutz der Clients beim Kunden durchführen und überprüfen.
Standardpaket:
Managed Anti-Virus beinhaltet die Bereitstellung von Anti-Virus-Lizenzen inklusive Wartungs-/Updatepakete durch den Auftragnehmer für den Client-Schutz des Kunden. Weiterhin erfolgt die regelmäßige Überprüfung, ob ein eine aktuelle Virensignatur auf dem Client im Einsatz ist. Dies erfolgt über die Prüfung der Aktualität der vom Softwarehersteller bereitgestellten Signaturen werktäglich um 9 Uhr; Beide Parteien vereinbaren, dass eine Alarmierung erfolgt, sobald eine Signatur älter als 1 Kalendertag sein sollte.
Premiumpaket:
Zusätzlich werden die gefundenen Viren in eine vom Auftragnehmer zentral verwaltete Quarantäne eingestellt. Sofern der Kunde eine Datei, die in die Quarantäne verschoben wurde, anfordert, erfolgt folgender Prozess: Der Techniker des Auftragnehmers analysiert die als gefährlich eingestufte Datei. Im Anschluss wird der Techniker dem Kunden einen unverbindlichen Vorschlag unterbreiten, ob die infizierte Datei zurück in den Produktivbetrieb gebracht werden kann. Der Kunde entscheidet über die Freigabe der Datei und wird hierzu eine E-Mail an den Auftragnehmer übermitteln.

9 Web-Filter
Präambel:
Ein 100%iger Schutz vor dem Zugriff auf schadhafte Webseiten ist nicht möglich. Der Auftragnehmer wird nach den üblichen Standards Maßnahmen zum Schutz der Clients beim Kunden durchführen und überprüfen. Es wird ein Web-Filter-System für die Clients des Kunden zur Verfügung gestellt. Es enthält die Funktion, unsichere Seiten nach vorbereiteten und redaktionell gepflegten Kategorien zu sperren, White- & Black-List-Einträge zu setzen. Die Erarbeitung und die systemtechnische Umsetzung einer Web-Richtlinie für den Kunden sowie etwaige spätere Änderungen an der Richtlinie und der White- & Blacklists werden nach Freigabe des Kunden gemäß Ziffer 15 abgerechnet.

10 USB-Gerätekontrolle
Das Premiumpaket enthält eine Funktion, durch die es möglich wird, die USB-Anschlüsse der Clients zu sperren, um dadurch möglichen Datendiebstahl zu verhindern. Zugelassene Ausnahmen für bestimmte Gerätetypen sind konfigurierbar.

11 Bereinigung von temporären Dateien und Eventlogeinträgen
Beim Standard- und Premiumpaket erfolgt eine regelmäßige Bereinigung (Standard: monatlich, Premium: wöchentlich) von temporären Dateien, des Browser-Cache (Flash, Java, Dateien), Terminalserver-Cache und Eventlogeinträgen inklusive Bereitstellung eines Berichts über den Erfolg der Maßnahme im IT-Management System.

12 Installation aktueller Sicherheitsupdates
Beim Standard- und Premiumpaket erfolgen die Bereitstellung und der Betrieb einer Software zur Schwachstellenanalyse und Installation aktueller Microsoft- und Drittanbieter-Sicherheitsupdates gemäß „Anlage 2 – Liste der unterstützten Software für das Patch-Management“. Der Auftragnehmer führt auf den Clients tägliche Installationsroutinen gemäß Anlage B „Installationsmethode für das Patch-Management“ zur Implementierung von Sicherheitsupdates durch und lässt Clients nach erfolgter Installation neu starten. Der Kunde ist mit diesem Prozess einverstanden und wird entsprechend notwendige Wartungsfenster für diese Maßnahmen einrichten. Die Sicherstellung der erfolgreichen Installation der Sicherheitsupdates erfolgt über eine tägliche Abfrageroutine, deren Ergebnis jederzeit im vom Auftragnehmer bereitgestellten IT-Management-System abgerufen werden kann. Ein monatlicher Bericht über den Erfolg der Sicherheitsupdates wird auf Wunsch / auf Anforderung des Kunden per E-Mail an den Kunden versendet.
Die Haftung für die Fehlerfreiheit der Sicherheitsupdates, die Sinnhaftigkeit der Risiko-Klassifizierung, sowie die Kompatibilitätseinschätzung mit der zu aktualisierenden Software liegt allein beim jeweiligen Softwarehersteller. Dem Kunden ist bewusst, dass Sicherheitsaktualisierungen Veränderungen an der installierten Software vornehmen um die Sicherheit oder Stabilität zu verbessern. Bei diesen Veränderungen kann es zu Problemen kommen, die die Lauffähigkeit des Systems negativ beeinflussen. Für Folgeschäden aus diesem Umstand übernimmt der Auftragnehmer keine Haftung. Der Auftragnehmer wird die Problemlösung nach üblichen Standards herbeiführen.

Standardpaket:
Der Kunde ist damit einverstanden, dass die vom Softwarehersteller veröffentlichten Sicherheitsupdates ohne vorherige Prüfung auf den Systemen installiert werden.
Sofern die zu versorgenden Geräte zum in Anlage B vereinbarten Zeitpunkt angeschaltet sind und über eine zuverlässige Internetverbindung verfügen sichert der Auftragnehmer die Installation der Updates innerhalb von zwei Wochen nach Erscheinen der Updates für die Clients des Kunden zu. Maßgebend für die Ermittlung des Erfolgs der Maßnahme ist der aus dem vom Auftragnehmer bereitgestellten Management-System abrufbare Monats-Bericht in der Kategorie „Patch-Management“. Sollten mehr als zwei fehlende Patches in dem Bericht verzeichnet sein, so ist der Kunde innerhalb von zwei Wochen nach Zugang des Berichts berechtigt, für jedes weitere fehlende Patch eine Gutschrift von 10% der Managed Service-Client-Monatsgebühr des betroffenen Geräts zu verlangen.

Premiumpaket:
Es erfolgen für die vom Softwarehersteller veröffentlichten Sicherheitsupdates zunächst eine Prüfung nach üblichen Standards in Bezug auf die Abhängigkeiten und Kompatibilitäten sowie eine Testinstallation auf einem vom Kunden zu benennenden produktiv genutzten Gerät. Sollte sich der Kunde innerhalb von einer Woche nicht mit erheblichen Störungen beim Auftragnehmer melden, gilt die Installation des Sicherheitsupdates auf alle weiteren Systeme als vom Kunden genehmigt. Für diese Tätigkeiten ist ein Dienstleistungs-Kontingent von 3min pro Monat pro Client enthalten, welches über alle Clients kumuliert wird. Sollte das gesamte Kontingent in einem Monat erschöpft worden sein, so erfolgt die Berechnung der weiteren Stunden gemäß Ziffer 15 nach Freigabe des Kunden.

13 Jährliches IT-Sicherheits-Coaching, individuell pro Mitarbeiter
Das Premiumpaket beinhaltet ein 15-minütiges individuelles Coaching auf Basis seines IT-Wissensstands pro Mitarbeiter pro Jahr. Vorab hat der Verantwortliche des Kunden die Möglichkeit, Einfluss auf die Inhalte des Gesprächs zu nehmen, indem er mindestens 4 Wochen vor der Durchführung dem Auftragnehmer seine Wünsche anzeigt. Die Themen für das Coaching umfassen die Sensibilisierung für Passwort-Sicherheit, die Sensibilisierung für Social-Engineering sowie aktuelle Bedrohungen (bspw. Crypto-Trojaner). Das IT-Sicherheits-Coaching wird auf Wunsch/Anfrage des Kunden durchgeführt und findet ausschließlich per Videokonferenz (Microsoft Teams) statt. Hierzu wird max. ein Coaching-Tag mit 15-minütigen Zeitslots für alle Mitarbeiter vereinbart.

14 Einrichtungsgebühr pro Client
Nachdem die Voraussetzungen zur Ist-Analyse gemäß „Voraussetzungen“ erfüllt sind, werden die Clients mit entsprechenden Agenten des IT-Management-Systems versehen und konfiguriert. Dieser Aufwand ist mit der Einrichtungsgebühr gemäß Bestellformular abgegolten. Bei einem Hinzufügen weiterer Clients zum Betreuungsumfang und/oder einem Hardwareaustausch innerhalb des Betreuungsumfangs fallen Tätigkeiten und Einrichtungsgebühr erneut im selben Umfang an.

15 Stundensatz für weitere Leistungen
Der Stundensatz für die Erbringung von Dienstleistungen wie technische Hilfestellung, Fehleranalyse, Lösungserarbeitung, Umsetzung und Dokumentation in der Zeit von Mo-Fr 7:00 – 18:00 Uhr gilt gemäß IT-Servicevereinbarung und der jeweils gültigen Preisliste. Abgerechnet wird im 15min-Takt.
Etwaige Fahrtkosten werden mit EUR 0,50 pro Entfernungskilometer berechnet. Die Anfahrtszeit wird mit dem vorgenannten Stundensatz abgerechnet, die Rückfahrtzeit wird nicht berechnet.
Ein Fernzugriff auf die Kundensysteme erspart dem Kunden die Fahrtkosten, die Zeit wird wie zuvor genannt abgerechnet.
Der Kunde ist damit einverstanden, dass aufgrund von Fehlermeldungen, die sich aus dem Monitoring der Clients nach Ziffer 3 ergeben, bis zu 15min pro Monat pro Client die notwendigen technischen Maßnahmen auf Basis der Vergütungsregelung in dieser Ziffer eingeleitet werden. Bei Buchung der Flatrate Optionen fallen hierfür keine zusätzlichen Kosten an.
Außerhalb des Zeitraums werden 50% Zuschlag (zwischen 18:00 – 7:00 Uhr) bzw. 100% Zuschlag (Sonntags- und Feiertags) berechnet.

16 Flatrate für Fernunterstützung

Die Maßnahmen zur angestrebten Störungsbeseitigung (ITIL-Klasse „Incident“) sind als Fernwartungs-Leistung pauschal enthalten und werden nicht nach Ziffer 15 abgerechnet. Administrationstätigkeiten (ITIL-Klasse „Service Request“) sind ebenfalls pauschal enthalten. Der Auftragnehmer behält sich vor, bei übermäßiger Nutzung im quartalsweisen Beratungsgespräch eine Anpassung dieses Elements vorzuschlagen.
Die Leistungen werden in der Zeit von Mo-Fr 7:00 – 18:00 Uhr erbracht.
System-, Software- oder Konfigurationsänderungen an den Clients dürfen nur durch den Auftragnehmer-Support durchgeführt werden. Dies bedeutet, dass die Administrationskennwörter nur beim Auftragnehmer für Systemzugriffe vorhanden sind. Der Kunde darf die Administrationskennwörter nur zur Notfallabsicherung in einem versiegelten Brief in seinem Tresor aufbewahren.
Die Flatrate für Störungsbeseitigungen und Administrationstätigkeiten bezieht sich auf technische Dienstleistungen, die am Betriebssystem sowie an weiteren Anwendungen & Diensten laut Anlage 1 durchgeführt werden. Weitergehende Tätigkeiten an Softwareprogrammen oder angeschlossenen bzw. verbundenen Geräten wie Drucker, USB-Speicher etc. sind nicht durch die Flatrate abgedeckt.
Änderungen des konfigurierten Standards (ITIL Klasse „Change Request“) sind grundsätzlich nicht in der Flatrate enthalten und werden gesondert angeboten. Der Auftragnehmer wird nach üblichen Standards die Problemlösungen an den Softwareprogrammen durchführen. Eine Haftung für einen fehlerfreien Betrieb kann nicht übernommen werden da dies nicht im Einflussbereich des Auftragnehmers, sondern in dem der jeweiligen Softwarehersteller liegt.

17 Gültigkeit Servicebedingungen

Nachrangig zu den Regelungen dieser Leistungsbeschreibung gelten die Servicebedingungen in der jeweils aktuellen Version. Außerdem gelten nachrangig für die eingesetzten Softwareprodukte die Lizenz- und Nutzungsbedingungen der jeweiligen Hersteller. Weiterhin gelten nachrangig die allgemeinen Geschäftsbedingungen, jederzeit abrufbar unter https://systemhaus-ruhrgebiet.de/service.

Anlage 1 – Liste der von der Flatrate abgedeckten Anwendungen & Dienste

Die Flatrate ist gültig für die im Folgenden genannten Anwendungen & Dienste sofern die Flatrate für den jeweiligen Client gebucht ist, auf dem die nachfolgenden Anwendungen & Dienste betrieben werden.

- Anwendungen & Dienste des Betriebssystems: DNS-Client, DHCP-Client, Druckdienste
- Microsoft Office & Microsoft 365
- Mozilla Firefox
- Google Chrome
- Adobe Reader, Foxit Reader
- PDF Creator
- IrfanView
- WinZip, WinRAR

Ausgeschlossen sind nicht genannte Drittanbieter-Anwendungen & -Dienste die mit den vorgenannten Anwendungen und Dienste verknüpft sind, auch wenn diese augenscheinlich zur Applikation gehören.

Anlage 2 – Liste der unterstützten Software für das Patch-Management

Die Liste der unterstützten **Microsoft-Software** ist jederzeit abrufbar unter https://systemhaus-ruhrgebiet.de/service

Nur Versionsstände der Microsoft-Software werden unterstützt, welche sich laut Microsoft in der Mainstream-Support oder Extended Support-Phase befinden. Unter http://support2.microsoft.com/lifecycle/search/ kann dies direkt beim Hersteller überprüft werden.
Es werden keine ServicePacks und kumulative Sicherheits-Updates unterstützt. Ausnahme: Für Windows 10 werden kumulative Updates unterstützt.

Die Liste der unterstützten **Drittanbieter-Software** ist jederzeit abrufbar unter https://systemhaus-ruhrgebiet.de/service

Nur Versionsstände der Drittanbieter-Software werden unterstützt, für welche laut jeweiligem Hersteller kostenlose Patches angeboten werden. Dies kann direkt beim Hersteller recherchiert werden.