

Postbeamtenkrankenkasse

Leistungsbeschreibung
Ausschreibung Managed Client 2027

Stand: 07.08.2026

Inhaltsverzeichnis

Inhaltsverzeichnis.....	2
Vorbemerkung	4
1 Allgemeine Informationen	5
1.1 Datenschutz	5
1.2 Geheimhaltung/Vertraulichkeit.....	5
1.3 Personal des AN	5
1.3.1 Datenschutz	5
1.3.2 Ausscheiden und Veränderung eines Mitarbeiters	5
1.4 Virenschutz	6
1.5 Anbindung Ticket System.....	6
2 Einleitung und Zielsetzung	7
2.1 Beschreibung der Ausgangssituation	7
2.2 Zielsetzung	7
2.3 Überblick Projektphasen.....	7
2.3.1 Abstimmung nach Zuschlag.....	7
2.3.2 Aufbau Infrastruktur	8
2.3.3 Rollout Hardware + Pilotbetrieb	8
2.3.4 Betrieb	8
3 Leistungsgegenstand	9
3.1 Hardware-Bereitstellung (Mietmodell).....	9
3.2 Betriebssystem-Installation und -Konfiguration	10
3.3 Patch- und Update-Management.....	10
3.4 Softwarepaketierung und -verteilung	11
3.5 Hardwareinventar	11
3.6 Security Services.....	11
3.7 Zugang zum Unternehmensnetzwerk	12
4 3. Service Level Agreement (SLA)	13
4.1 Servicepaket	13
4.2 Reaktions- und Lösungszeiten	13
4.3 Priorisierung	13
5 Schnittstellen zu Managed Services.....	15
5.1 Schnittstelle Managed LAN	15
5.2 Schnittstelle Managed VPN	15
5.3 Schnittstelle Managed Active Directory	15

5.4 Schnittstelle zum Security Operation Center	15
5.5 Schnittstellenmatrix	16
6 Betriebsprozesse	17
6.1 Lifecycle-Management	17
6.2 Incident Management	17
6.3 Change Management	17
6.4 IMAC/D-Leistungen	17
7 Monitoring und Reporting	19
7.1 Client-Monitoring	19
7.2 Berichtswesen	19
8 Rahmenbedingungen	20
8.1 Vertragslaufzeit und Kündigung	20
8.2 Datenschutz und Informationssicherheit	20
8.3 Umgang mit nichtflüchtigen Speichermedien	20
8.4 Green-IT und Nachhaltigkeit	20
9 Mitwirkungspflichten der Auftraggeberin	21
10 Optionale Leistungen	22
10.1 Unterstützung vor Ort	22
10.1.1 Erstinstallation von Clients	22
10.1.2 Außerbetriebnahme von Clients	22
10.2 Softwarepaketierung	23
11 Hinweise zur Bepreisung der Leistungen	24
11.1 Standardleistungen	24
11.2 Optionale Leistungen	24
12 Anhänge	25
12.1 Leistungsverzeichnis Hardware (LV-Hardware) mit technischen Spezifikationen je Gerätekategorie	25
12.2 Standard-Softwarekorb	27
12.3 Übersicht der anzupassenden BIOS-Einstellungen	27

Vorbemerkung

In diesem Dokument sind die Regelungen der Leistungsbeschreibung zur Ausschreibung „Managed Client 2027“ festgelegt.

Die Leistungsbeschreibung regelt im Detail die Leistungspflichten und Mitwirkungsobliegenheiten der Vertragspartner. Im Rahmen der Ausschreibung ist sie Bestandteil des Vertrags zwischen der Auftraggeberin „Postbeamtenkrankenkasse“ bzw. „PBeaKK“ und dem Auftragnehmer („AN“).

Soweit nicht ausdrücklich anders geregelt, haben die nachfolgend verwendeten Begriffe eine Bedeutung wie im Vertragstext vorgesehen.

1 Allgemeine Informationen

1.1 Datenschutz

Die Vertragspartner beachten die jeweils geltenden Rechtsvorschriften des Datenschutzes. Eine Erhebung, Verarbeitung und Nutzung der Daten für andere als die vertraglich vereinbarten Zwecke ist nicht zulässig. Eine Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz findet nicht statt. Verstöße gegen den Datenschutz sind dem jeweiligen Vertragspartner unverzüglich zu melden, ebenso unverzüglich ist Abhilfe zu schaffen. Die Auftraggeberin ist für die Beurteilung der Zulässigkeit der Datenverarbeitung und die eventuelle Wahrung der Rechte von Betroffenen (z.B. Mitgliedern, mitversicherten Angehörigen) verantwortlich.

Die Protokollierung und Speicherung von Inhaltsdaten bedarf in jedem Einzelfall der Genehmigung der AG.

Nicht genehmigungspflichtig sind Protokollierungen und Auswertungen, die dem Zweck Sicherstellung der Leistungserbringung dienen und bei denen keine inhaltlichen Daten protokolliert oder ausgewertet werden, sondern nur Untersuchungen zu Datenmenge, Datenrichtung und Funktionsfähigkeit durchgeführt werden. Hierbei ist eine Personenbeziehbarkeit zu unterlassen.

Es gelten die ergänzenden Datenschutzbestimmungen gemäß Anlage 8c der Vergabeunterlagen. Diese wird auch Vertragsbestandteil.

1.2 Geheimhaltung/Vertraulichkeit

Der Auftragnehmer verpflichtet sich alle ihm im Rahmen des Auftrags zur Verfügung gestellten sowie direkt oder indirekt zur Kenntnis gekommenen personenbezogenen und geschäftskritischen Daten, Informationen und Unterlagen strikt vertraulich zu behandeln, diese ausschließlich zur Auftragserfüllung zu verwenden, und diese nicht ohne vorherige schriftliche Zustimmung des Auftraggebers an Dritte weiterzugeben, zu verwerten oder zu verwenden. Die Mitnahme von Unterlagen ist untersagt, es sei denn, der Auftragsinhalt sieht dies vor und eine Vereinbarung gestattet dies ausdrücklich.

1.3 Personal des AN

1.3.1 Datenschutz

Der AN muss seine Mitarbeiter auf die Einhaltung der einschlägigen Gesetze und Vorschriften für Datenschutz und -sicherheit sowie der internen sicherheitsrelevanten Regelungen des AN verpflichten.

1.3.2 Ausscheiden und Veränderung eines Mitarbeiters

Der AN ist verpflichtet, beim Ausscheiden oder bei der Veränderung eines Mitarbeiters sämtliche für den Mitarbeiter eingerichteten Zugangsberechtigungen und Zugriffsrechte sofort zu löschen bzw. ihm zu entziehen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen. Der AN dokumentiert revisionsfähig die vergebenen Zugriffsrechte. Die Dokumentation ist für einen Zeitraum von 24 Monaten vorzuhalten und ist den AG auf Verlangen unverzüglich vorzulegen.

Der AN stellt sicher, dass Zugangsberechtigungen zu IT-Systemen, die mit mehreren Personen geteilt wurden (z. B. mittels eines gemeinsamen Passwortes), nach Ausscheiden bzw. Veränderung einer dieser Personen sofort geändert werden. Außerdem sind durch den AN sämtliche mit Sicherheitsaufgaben betrauten Personen der AG – die im Rahmen der Abstimmung festgelegt und dem AN benannt werden - über das Ausscheiden bzw. die Veränderung des Mitarbeiters zu unterrichten.

1.4 Virenschutz

Der AN ist verpflichtet, auf allen Systemen, die er im Zusammenhang mit den Systemen der AG nutzt, dem jeweils aktuellen Stand der Technik entsprechende Maßnahmen gegen Virenbefall oder sonstige Schädlinge (Trojaner, Bomben etc.) zu treffen. Die Erfüllung der folgenden organisatorischen Maßnahmen ist hierzu notwendig:

Nur auf Viren überprüfter Inhalt von Wechseldatenträgern darf auf feste Speichermedien kopiert werden.

E-Mails müssen auf den Systemen vor deren Öffnung auf Viren überprüft werden.

Darüber hinaus stellt der AN sicher, dass alle Systeme einen geeigneten Virenschutz haben. Der AN wird Vorkehrungen treffen, um die regelmäßige Aktualisierung der Virenschutzsoftware sicherzustellen.

Beim Auftreten oder beim dringenden Verdacht eines die AG betreffenden Virenbefalls ist der AN verpflichtet, den Vorfall der AG sofort nach Kenntniserlangung telefonisch oder per Fax zu melden und dazu, soweit möglich, folgende Angaben zu machen:

- Um welchen Virus handelt es sich? (Name/Version)
- Woher kam der Virus? (bekannt/vermutet/unbekannt)
- Wie wurde er erkannt? (Virens Scanner: Name/Version/Version der Virensignaturdatenbank)
- Wurde er beseitigt? (ja/nein/unbekannt)
- Wurde er an andere Stellen verteilt? (ja/nein/unbekannt)
- Wenn ja - wohin und wie (Diskette/ftp/E-Mail etc.)

1.5 Anbindung Ticket System

Der AN muss über ein Trouble-Ticket-System verfügen, dass den elektronischen Datenaustausch mit den TTS der AG realisieren kann. Der AG muss es möglich sein, die Störungsmeldungen an das TTS des AN zu senden. Der Empfang ist zu quittieren. Der Datenaustausch soll über eine Emailkoppelung realisiert werden, wobei der AN bei Rückmeldungen auf die Ticketnummer der AG referenzieren muss.

2 Einleitung und Zielsetzung

2.1 Beschreibung der Ausgangssituation

Die Postbeamtenkrankenkasse (PBeaKK) ist eine Sozialeinrichtung der früheren Deutschen Bundespost in der Rechtsform einer bundesunmittelbaren rechtsfähigen Körperschaft des öffentlichen Rechts mit Selbstverwaltung.

Die PBeaKK gewährt ihren Versicherten (Mitgliedern und mitversicherten Angehörigen) nach Maßgabe ihrer Satzung Leistungen in Krankheits- und Geburtsfällen. Daneben berechnet und zahlt sie ihren Mitgliedern im Auftrag der jeweiligen Dienstherrn Beihilfeleistungen nach der Bundesbeihilfeverordnung (BBhV). Sie handelt insoweit öffentlich-rechtlich. Darüber hinaus führt die PBeaKK im Auftrag der Gemeinschaft privater Pflegeversicherer für ihre Versicherten die private Pflegepflichtversicherung nach dem Pflege-Versicherungsgesetz durch.

Die Postbeamtenkrankenkasse ist daher weder eine gesetzliche Krankenkasse, noch ein privates Krankenversicherungsunternehmen.

2.2 Zielsetzung

Die vorliegende Leistungsbeschreibung definiert den Umfang, die Qualitätsanforderungen und die organisatorischen Rahmenbedingungen des Managed Service "Managed Client 2027". Der Service umfasst die Bereitstellung, den Betrieb und die Verwaltung von IT-Arbeitsplatzendgeräten als vollständig gemanagten Service.

Ziel ist die Entlastung der internen IT-Organisation der Auftraggeberin durch die Übernahme aller betriebsrelevanten Aufgaben rund um den Client-Arbeitsplatz. Die Auftraggeberin erhält einen stets aktuellen, sicheren und leistungsfähigen IT-Arbeitsplatz zu planbaren monatlichen Kosten.

Der Managed Client ist integraler Bestandteil des Managed Services Portfolios des Auftragnehmers und weist definierte Schnittstellen zu den Services Managed LAN, Managed Active Directory und dem Security Operation Center auf.

Zur Unterstützung der AG bei Rollout oder in Urlaubszeiten wird optional Vor-Ort Support benötigt.

2.3 Überblick Projektphasen

Die Einführung des „Managed Client 2027“ soll in drei Phasen durchgeführt werden:

Phase 1: Abstimmung	nach Vertragsschluss
Phase 2a: Aufbau Infrastruktur	01.02.2027
Phase 2b: Rollout HW + Pilotbetrieb	01.03.2027
Phase 3: Betrieb	01.04.2027

2.3.1 Abstimmung nach Zuschlag

Während der Abstimmungsphase sind insbesondere folgende Punkte zu klären:

- Die Feinabstimmung von Betriebsprozessen zwischen AG und AN
- Die Vorbereitung der Phase Aufbau und Pilotbetrieb, indem die für den Betriebsübergang notwendigen Maßnahmen festgelegt werden und die Konfigurationsdaten für den Aufbau definiert werden

- Abstimmung der einzelnen Arbeitsanweisungen und Vorgaben
- Abstimmung der Details für den Pilotbetrieb

2.3.2 Aufbau Infrastruktur

Nach der Abstimmungsphase übernimmt der AN die technische Umsetzung und gewährleistet, dass alle Systeme korrekt miteinander kommunizieren. Hierbei sind sowohl die Schnittstellen zu anderen Managed Services zu implementieren als auch die ausgeschriebene Lösung zur Verwaltung aller Clients zu realisieren.

2.3.3 Rollout Hardware + Pilotbetrieb

Die Hardware wird vom AN verpackungsfrei in Stuttgart angeliefert, optional stellt der AN Mitarbeiter zur Verfügung, die die AG bei der Auslieferung bzw. der Migration unterstützen.

Die AG plant, die Auslieferung der Geräte bis Ende März abzuschließen.

Die ausgeschriebene Lösung zur Verwaltung aller Clients ist funktionsfähig, insbesondere Patches und Updates müssen erfolgen können.

Eine Rücknahme von Altgeräten der AG ist nicht Bestandteil der Leistung.

2.3.4 Betrieb

Nach Abnahme der Lösung übernimmt der AN die Betriebsverantwortung für die nach den Maßgaben und Service Leveln des Leistungsverzeichnisses bzw. den vereinbarten Prozessen und Arbeitsanweisungen (Servicehandbuch).

Der AN übernimmt die Gesamtverantwortung für die Verwaltung der Clients. Dies umfasst das Incident Management, das Management von Service Requests sowie den Betrieb der Clients nach den definierten Prozessen.

Der AN hat zum Ende der Vertragslaufzeit sicherzustellen, dass alle für einen eventuellen Wechsel zu einem neuen Anbieter notwendigen Informationen und Dokumentationen bei der AG vorliegen. Darüber hinaus ist der AN verpflichtet, ohne zusätzliche Vergütung den Wechsel in angemessener Weise zu unterstützen, um so einen möglichst reibungsfreien Übergang zu ermöglichen.

3 Leistungsgegenstand

Der Managed Client umfasst die folgenden Kernleistungen als Gesamtpaket:

3.1 Hardware-Bereitstellung (Mietmodell)

Die Bereitstellung der Endgeräte erfolgt im Rahmen eines Mietmodells über eine Laufzeit von 36 Monaten. Die Hardware verbleibt im Eigentum des Auftragnehmers. Nach Ablauf der Mietlaufzeit erfolgt ein geregelter Gerätetausch inklusive zertifizierter Datenlöschung und fachgerechter Entsorgung der Altgeräte.

Geräteportfolio: Das Portfolio umfasst standardisierte Geräteklassen, die auf die typischen Anforderungsprofile der Arbeitsplätze abgestimmt sind:

Gerätekategorie	Beschreibung	Einsatzbereich
Desktop Performance	Erweiterte Konfiguration mit höherer CPU-/RAM-Ausstattung für anspruchsvolle Anwendungen	Entwicklung, Datenanalyse
Notebook Standard	Mobiler Arbeitsplatz mit Dockingstation-Fähigkeit	Mobiles Arbeiten, Home-office, Besprechungen
Notebook Performance	Erweiterter mobiler Arbeitsplatz mit größerem Bildschirm und GPU-Unterstützung	Entwicklung, Datenanalyse
Docking Station	Herstellerspezifische Docking Station mit Ein-/Ausschalter für die Laptops	Mobiles Arbeiten
Mobiltelefon Standard	Mobiltelefon mit ausreichender Leistung für Mail, Telefonie und Browser	Bereitschaft
Mobiltelefon Erweitert	Mobiltelefon mit ausreichender Leistung für Mail, Telefonie und Browser und erweitertem Bildschirm	Bereitschaft
Tablet	Tablet mit Ausreichende Leistung für Mail, Browser	Schulungen

Alle bereitgestellten Geräte tragen die CE-Kennzeichnung, erfüllen die aktuellen Energieeffizienzanforderungen und verfügen über eine Herstellergarantie über die gesamte Mietlaufzeit. Die Hardware-Spezifikationen werden in einem separaten Leistungsverzeichnis (Anlage A: LV-Hardware) je Gerätekategorie technisch detailliert beschrieben.

Für alle gelieferten Geräte ist vom AG eine Sicherheitsprüfung nach DGUV vor Auslieferung durchzuführen.

Zur Abdeckung von HW-Defekten wird die AG für die Gerätekategorien Standard einen Pool von Austauschgeräten in Stuttgart vorzuhalten, der im Falle eines HW-Defektes genutzt wird, um

den betroffenen Anwender schnell mit einem Ersatzgerät zu versorgen. Die defekten Geräte werden in der HV in Stuttgart gesammelt und an den Auftragnehmer zur Reparatur gesandt.

Die AG stellt dem AN Inventar Labels zum Ausdruck bereit, die vor Auslieferung vom AN anzubringen sind. Vor der Lieferung der Geräte stellt der AN eine Liste der gelieferten Geräte mit Seriennummer und Inventarlabelnummern bereit.

Der Lieferung muss verpackungsfrei in die Zentrale nach Stuttgart erfolgen.

3.2 Betriebssystem-Installation und -Konfiguration

Jedes Endgerät wird vor der Auslieferung mit dem zum Lieferzeitpunkt aktuellsten, vom Hersteller unterstützten Betriebssystem installiert und konfiguriert. Aktuell ist dies Windows 11 Enterprise in der 64-Bit-Version bzw. iOS für die Mobilgeräte

Die Installation umfasst:

- Automatisierte Erstinstallation (Zero-Touch Deployment) über die zentrale Softwareverteilung
- Domänenbeitritt/Hybrid Join und Anwendung der unternehmensspezifischen Richtlinien bzw. Gruppenrichtlinien (in Abstimmung mit Managed AD) für Windows 11
- Konfiguration der Sicherheitsrichtlinien gemäß Vorgaben des Managed Security Service
- Aktivierung der Festplattenverschlüsselung (BitLocker) mit zentraler Schlüsselverwaltung für Windows 11 und deren Speicherung in Active Directory oder Verwaltung System.
- Installation aller zum Lieferzeitpunkt aktuellen Sicherheits- und Funktionsupdates
- Installation der unternehmensspezifischen Basissoftware gemäß definiertem Standard-Softwarekorb

Der Einsatz von M365 Apps für Enterprise ist aus Datenschutzgründen bei der AG nicht möglich.

3.3 Patch- und Update-Management

Das Patch- und Update-Management stellt die kontinuierliche Aktualität und Sicherheit aller verwalteten Clients sicher. Die Leistung umfasst:

Sicherheitsupdates (Security Patches): Bereitstellung und gesteuerte Installation sicherheitsrelevanter Updates des Betriebssystemherstellers. Kritische Sicherheitspatches (CVSS ≥ 7.0) werden innerhalb von 24 Stunden nach Freigabe durch den Hersteller zur Verteilung bereitgestellt. Die Verteilung erfolgt in definierten Wartungsfenstern, um den laufenden Betrieb nicht zu beeinträchtigen. Für Windows 11 werden Patches in unterschiedlichen Ringen ausgerollt. 48 Stunden nach der Freigabe durch den Hersteller wird der erste Ring ausgerollt. Der allgemeine Rollout erfolgt 7 Tage später.

Funktionsupdates: Qualitätsupdates und Feature-Updates des Betriebssystems werden nach vorheriger Freigabe durch den Auftragnehmer in einem abgestimmten Zeitplan ausgerollt. Vor der Verteilung erfolgt ein Test auf Kompatibilität mit der eingesetzten Fachanwendungslandschaft. Die AG plant ein jährliches Feature-Update.

Firmware- und Treiber-Updates: BIOS/UEFI- und Treiber-Updates werden herstellerekonform über die jeweilige Management-Lösung des Hardware-Herstellers bereitgestellt und zentral verteilt. Eine Liste der vom AN durchzuführenden BIOS-Einstellungen findet sich im Anhang.

Third-Party-Patchmanagement: Für definierte Standard-Drittanbieter-Software (z. B. Adobe Reader, Browser, Java, 7-Zip) werden Sicherheitsupdates ebenfalls zentral bereitgestellt und installiert.

Das Patch-Management wird monatlich in einem Statusbericht dokumentiert, der die Patch-Compliance-Rate, offene Patches und eventuelle Ausnahmen ausweist.

3.4 Softwarepaketierung und -verteilung

Der Auftragnehmer übernimmt die Paketierung, Qualitätssicherung und Verteilung von Anwendungssoftware auf die verwalteten Clients:

Paketierung: Erstellung von Installationspaketen nach standardisierten Methoden (MSI/MSIX, Skriptbasiert) für die zentrale Softwareverteilung. Jedes Paket durchläuft eine Qualitätssicherung auf einer Referenzumgebung vor der produktiven Freigabe.

Standard-Softwarekorb: Definition und Pflege eines Standard-Softwarekorbs, der die Basissoftware aller Arbeitsplätze umfasst (Office-Suite, Browser, PDF-Reader, Kommunikations-tools, Fachverfahren gemäß Vereinbarung).

Softwareverteilung: Automatisierte, zeitgesteuerte oder anlassbezogene Verteilung von Software auf die Zielgeräte. Die Verteilung erfolgt bandbreitenoptimiert und kann für definierte Gerätegruppen oder einzelne Geräte erfolgen.

Self-Service-Portal: Bereitstellung eines Self-Service-Portals, über das Anwender und Anwenderinnen optional freigegebene Software für Windows eigenständig anfordern und im lokalen „Userspace“ installieren können (Company Portal / Software Center).

Die Anwender und Anwenderinnen haben die Berechtigung eigene iOS-Apps aus dem App-Store des Herstellers Apple zu installieren, allerdings gibt es eine Blacklist für nicht erlaubte Apps. Zusätzlich ist ein kundenspezifischer zentraler App-Store bereitzustellen, in dem Standard Apps der Auftraggeberin (z.B. WebEx) bereitgestellt werden.

Alle im Anhang 12.2 Standard-Softwarekorb aufgeführten Softwarepakete sind über die Vertragslaufzeit in aktueller Version bereitzustellen.

3.5 Hardwareinventar

Der AN stellt monatlich eine Übersicht aller gelieferten bzw. verwalteten Geräte bereit.

3.6 Security Services

Der Security Service verantwortet die clientspezifische IT-Sicherheitsstrategie. Die Aufgaben umfassen:

- Bereitstellung und Verwaltung der Endpoint Protection (Antivirus/EDR/XDR) auf allen verwalteten Windows Clients
- AN ist verantwortlich für Funktionsfähigkeit und Aktualität der Security Lösung
- Zentrale Steuerung der Festplattenverschlüsselung (BitLocker) mit Schlüsselhinterlegung
- Durchsetzung der Security-Baseline-Konfigurationen auf Betriebssystemebene
- Koordinierte Reaktion bei sicherheitsrelevanten Vorfällen (Security Incidents) am Client-Endpunkt
- Bereitstellung einer Möglichkeit für die AG einzelne Clients zu isolieren

- Bereitstellung von Compliance-Reports zur Endpoint-Sicherheit (Verschlüsselungsstatus, Patch-Stand, AV-Signaturaktualität)
- Integration in SIEM-/SOC-Infrastruktur durch Bereitstellung relevanter Client-Logdaten

3.7 Zugang zum Unternehmensnetzwerk

Für den Zugang zum Unternehmensnetzwerk für die Endgeräte mit einem Windows Betriebssystem der Managed VPN Service genutzt (siehe unten). Für die Endgeräte mit iOS ist ein Gateway zu unternehmensinternen Webdiensten und dem unternehmensinternen Mail-Service (Exchange) bereitzustellen. Die Liste der internen Webdienste unterliegt Änderungen (aktuell 10 Stück) mit zwei Änderungen pro Jahr. Die Konfiguration der Webdienste obliegt dem Auftragnehmer.

4 3. Service Level Agreement (SLA)

4.1 Servicepaket

Kriterium	Standard
Servicezeiten	Mo-Fr 08:00-17:00
Reaktionszeit Störung (normal)	Nächster Werktag
Reaktionszeit Service Request	2 Werktage
Wiederherstellzeit remote	Nächster Werktag
Wiederherstellzeit HW-Störung	2 Wochen ab Eingang HW beim AN
Patch-Compliance-Ziel	>= 90 %
Monitoring-Intervall	60 Minuten
Statusberichte	Monatlich
Quartalsweise Strategie-Review	Optional

4.2 Reaktions- und Lösungszeiten

Reaktionszeit: Zeitraum zwischen Eingang der Störungsmeldung im Ticketsystem und Beginn der qualifizierten Bearbeitung (Entgegennahme, Ersteinschätzung, Einleitung geeigneter Maßnahmen).

Wiederherstellzeit: Zeitraum zwischen Beginn der Bearbeitung und Wiederherstellung der Arbeitsfähigkeit des Anwenders.

Die Messung der SLA-Einhaltung erfolgt monatlich. Eine SLA-Zielerreichung von unter 95 % (Standard) über ein Kalenderquartal löst die in der Rahmenvereinbarung definierten Eskalations- und Kompensationsregelungen aus.

4.3 Priorisierung

Priorität	Definition	Beispiel
Hoch	Wesentliche Funktionseinschränkung, Workaround möglich	Anwendung stürzt ab, Drucker nicht erreichbar
Normal	Einzelne Funktion eingeschränkt, Produktivität kaum beeinträchtigt	Softwarefehler ohne Arbeitsstillstand

Niedrig	Wunsch, Optimierung, Informationsanfrage	Softwareinstallation, Konfigurationsänderung
----------------	--	--

5 Schnittstellen zu Managed Services

Der Managed Client ist als Baustein im Managed Services Ökosystem des Auftragnehmers konzipiert. Die Zusammenarbeit mit den angrenzenden Managed Services erfolgt über definierte Schnittstellen und gemeinsame Prozesse.

5.1 Schnittstelle Managed LAN

Der Managed LAN Service stellt die Netzwerkinfrastruktur für die Desktop und Notebook Rechner bereit, in die sich die verwalteten Clients integrieren. Die Schnittstelle umfasst:

- Bereitstellung und Konfiguration der LAN-/WLAN-Ports für neue Clients (Portfreischaltung, VLAN-Zuweisung)
- Netzwerkd Diagnose bei Konnektivitätsproblemen am Client (gemeinsame Fehleranalyse zwischen Client- und Netzwerkteam)
- Übergabe relevanter Netzwerkparameter (DNS, DHCP-Bereiche, Gateway) an das Client-Management
- Gemeinsames Monitoring der Netzwerkerreichbarkeit der Clients als Bestandteil der Verfügbarkeitsüberwachung

5.2 Schnittstelle Managed VPN

Der Managed VPN Service stellt den Zugang für die Windows basierten Notebooks in das Firmennetzwerk der AG bereit. Die hierbei genutzte Software (aktuell Cisco Secure Client VPN) wird durch die AG beigestellt.

5.3 Schnittstelle Managed Active Directory

Der Managed Active Directory Service bildet die zentrale Identitäts- und Zugriffsverwaltung. Die Schnittstelle umfasst:

- Automatisierter Domänenbeitritt neuer Windows Clients über die Deployment-Pipeline
- Anwendung und Durchsetzung von Gruppenrichtlinien (GPOs) auf den verwalteten Windows Clients
- Benutzer- und Berechtigungsverwaltung in Abstimmung mit dem Client-Team bei rollenbasierten Softwarezuweisungen
- Verwaltung von Computer-Konten und Organisationseinheiten (OUs) für das Client-Management

5.4 Schnittstelle zum Security Operation Center

Das Security Operation Center überwacht den Status aller Endgeräte der Auftraggeberin 24/7. Bei einem begründeten Verdachtsfall werden die für den Betrieb verantwortlichen Organisationseinheiten informiert und müssen entsprechend abgestimmte Maßnahmen wie die Isolation des Endgeräts durchführen.

5.5 Schnittstellenmatrix

Prozess / Aktivität	Managed Client	Managed LAN	Managed AD	Security Operations Center
Neuer Arbeitsplatz einrichten	Verantwortlich	Mitwirkung	Mitwirkung	-
Domänenbeitritt / GPO	Durchführung	–	Verantwortlich	–
Endpoint Protection	Verantwortlich	–	–	Information
Netzwerkonnektivität	Meldung	Verantwortlich	–	–
Patchmanagement	Verantwortlich	–	–	Freigabe/Audit
Sicherheitsvorfall am Client	Erstreaktion	–	–	Verantwortlich
Softwareverteilung	Verantwortlich	–	Mitwirkung	–
Inventarisierung / CMDB	Datenlieferung			–

6 Betriebsprozesse

6.1 Lifecycle-Management

Der gesamte Lebenszyklus eines verwalteten Clients wird durch den Auftragnehmer gesteuert:

Beschaffung und Bereitstellung: Auswahl und Beschaffung der Hardware gemäß den definierten Geräteklassen. Vorhaltung eines Pufferbestands zur Sicherstellung schneller Gerätebereitstellung.

Staging und Deployment: Vorkonfiguration der Geräte (Betankung) mit Betriebssystem, Treibern, Sicherheitskonfiguration und Standard-Softwarekorb. Auslieferung an den Einsatzort mit Inbetriebnahme vor Ort oder per Remote-Deployment.

Betrieb: Laufende Verwaltung, Patchmanagement, Monitoring, Störungsbeseitigung und Inventarisierung über die gesamte Mietlaufzeit von 36 Monaten.

Gerätetausch: Geplanter Austausch nach Ablauf der 36 Monate. Zertifizierte Datenlöschung (gemäß BSI-Vorgaben) oder physische Zerstörung der Datenträger. Fachgerechte Entsorgung oder Weiterverwendung der Altgeräte.

Produktinnovation: Während der Vertragslaufzeit werden Nachfolgemodelle in Abstimmung mit der Auftraggeberin evaluiert und eingeführt. Modelländerungen werden rechtzeitig angekündigt, um Kompatibilitätstests und Image-Anpassungen durchführen zu können.

6.2 Incident Management

Störungen am Client-Arbeitsplatz werden über das zentrale Ticketsystem der Auftraggeberin erfasst, klassifiziert und bearbeitet. Der Prozess folgt den ITIL-Vorgaben:

- Störungsmeldung durch Anwender über Hotline, E-Mail, Self-Service-Portal oder automatisierte Monitoring-Alerts
- Erstanalyse und Kategorisierung durch den 1st Level Support der PBeaKK
- Eskalation an den 2nd Level Support (Client-Spezialisten) bei nicht sofort lösbaren Störungen
- Remote-Fehlerbehebung durch den AN
- Bei Hardwaredefekten stellt die AG ein Austauschgerät aus dem HW-Pool zur Verfügung, anschließend erfolgt der Versand des defekten Gerätes an der AN
- Dokumentation aller Maßnahmen im Ticketsystem und Abschluss nach Bestätigung der Wiederherstellung

6.3 Change Management

Änderungen an der Client-Umgebung (z. B. neue Software, Konfigurationsänderungen, Betriebssystem-Upgrades) werden über den Change-Management-Prozess gesteuert. Änderungen werden nach Auswirkung und Risiko klassifiziert. Standard-Changes (z. B. Softwareinstallation aus dem Standardkorb) werden über vordefinierte Prozesse ohne individuelle Genehmigung abgewickelt. Normale und größere Changes durchlaufen ein Genehmigungsverfahren.

6.4 IMAC/D-Leistungen

Folgende Einzelleistungen sind über standardisierte Leistungsscheine abrufbar:

Leistung	Beschreibung
Install	Lieferung von vorkonfigurierten Geräten inkl. Peripherie
Delete	Deinstallation, zertifizierte Datenlöschung, Rückführung des Gerätes (in aller Regel nur bei Vertragsende)

Die Lösung des AN muss der AG die Möglichkeit bieten, eigenständig Geräte mit dem Betriebssystem neu zu betanken. Aus Sicht der AG ist hierzu eine SCCM-Lösung zu implementieren und mit der zentralen Verwaltungskomponente (z.B. Intune) zu verknüpfen. Die USB-Ports der AG sind aus Sicherheitsgründen für die Nutzung von USB-Sticks oder Festplatten gesperrt, daher ist eine Installation über USB nicht möglich.

7 Monitoring und Reporting

7.1 Client-Monitoring

Alle verwalteten Clients werden kontinuierlich überwacht. Das Monitoring umfasst die Aktualität der Antivirensignaturen, Patch-Compliance-Status sowie den Verschlüsselungsstatus der Datenträger. Im Fehlerfall erfolgt eine automatisierte Alarmierung an das Service-Team des Auftragnehmers.

7.2 Berichtswesen

Das regelmäßige Berichtswesen umfasst:

- Monatlicher Statusbericht: Gerätebestand, SLA-Kennzahlen, Patch-Compliance, Incident-Statistik, offene Maßnahmen
- Inventarbericht: Vollständige Auflistung aller verwalteten Geräte und installierter Software
- Security-Compliance-Report: Verschlüsselungsstatus, AV-Status, Patch-Stand (in Abstimmung mit Managed Security)
- Quartals-Review: Gemeinsame Bewertung der Servicequalität, Kapazitätsplanung und Optimierungsmaßnahmen

8 Rahmenbedingungen

8.1 Vertragslaufzeit und Kündigung

Die Hardware-Mietlaufzeit beträgt 36 Monate je Gerät. Der Managed Service Vertrag hat eine Laufzeit von 36 Monaten.

Für Nachbestellungen während der Vertragslaufzeit gilt das Enddatum des Vertrags. Für Nachbestellungen ist vom AN eine Formel anzugeben, nach der die evtl. höheren HW-Mieten der nachbestellten Geräte zu berechnen sind.

8.2 Datenschutz und Informationssicherheit

Der Auftragnehmer verpflichtet sich zur Einhaltung aller relevanten Vorgaben der DSGVO und des BDSG. Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Rahmen der vertraglich vereinbarten Leistungen. Ein Vertrag zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO ist Bestandteil der Rahmenvereinbarung.

Alle eingesetzten Mitarbeiter des Auftragnehmers werden auf das Datengeheimnis verpflichtet. Die Leistungserbringung erfolgt nach anerkannten Standards (ISO 27001, ITIL, BSI IT-Grundschutz). Sicherheitsüberprüfungen der eingesetzten Mitarbeiter werden auf Anforderung durchgeführt.

8.3 Umgang mit nichtflüchtigen Speichermedien

Nichtflüchtige Speichermedien (Festplatten, SSDs) werden bei Geräterückgabe, Reparatur oder Entsorgung gemäß den Vorgaben des BSI zertifiziert gelöscht. Über jede Löschung wird ein Löschzertifikat ausgestellt. Bei nicht ansprechbaren Speichermedien erfolgt eine mechanische Zerstörung. Bei Apple-Geräten reicht eine Rücksetzung auf den Auslieferungszustand.

8.4 Green-IT und Nachhaltigkeit

Der Auftragnehmer berücksichtigt bei der Gerätebeschaffung Energieeffizienzkriterien und bevorzugt Hardware mit entsprechenden Umweltzertifizierungen. Verpackungsmaterial wird auf das notwendige Minimum beschränkt und fachgerecht entsorgt. Altgeräte werden nach zertifizierter Datenlöschung einer Wiederverwendung oder fachgerechten Entsorgung zugeführt.

9 Mitwirkungspflichten der Auftraggeberin

Zur Sicherstellung einer reibungslosen Leistungserbringung ist die Auftraggeberin insbesondere zu folgenden Mitwirkungen verpflichtet:

- Bereitstellung der notwendigen Netzwerkinfrastruktur (Internetanbindung, LAN-Ports, Steckdosen) am Einsatzort
- Benennung fester Ansprechpartner für organisatorische und technische Abstimmungen
- Bereitstellung aller erforderlichen Zugänge und Berechtigungen für die Leistungserbringung
- Rechtzeitige Information über geplante organisatorische Änderungen (Umzüge, Personalveränderungen, Standortänderungen)
- Unterlassung nicht abgestimmter Änderungen an den verwalteten Geräten (keine eigenmächtige Software-Installation oder Hardware-Manipulation)
- Mitwirkung bei der Störungsanalyse und Bereitstellung relevanter Informationen bei Incidents
- Freigabe von Change-Requests innerhalb der vereinbarten Fristen
- Ggfs. Bereitstellung virtueller Server (für SW-Verteilung o.ä.)
- Ggfs. Bereitstellung eines VPN-Zugangs
- Im Falle von HW-Defekten übernimmt die AG den Austausch der Geräte aus dem Poolbestand und die Rücksendung der defekten Geräte an den AN
- Beistellung von Lizenzen Windows EMS E5
- Bereitstellung des Microsoft Tenants der AG im notwendigen Umfang

Sofern erforderliche Mitwirkungsleistungen nicht oder nicht rechtzeitig erbracht werden, kann dies zu Verzögerungen in der Leistungserbringung führen, die nicht zu Lasten des Auftragnehmers gehen.

10 Optionale Leistungen

10.1 Unterstützung vor Ort

Folgende Leistungen sollen auf Basis von T&M erbracht werden

10.1.1 Erstinstallation von Clients

Die Erstinstallation umfasst auf Basis der beschafften Hardware grundsätzlich folgende Leistungen vor Ort:

- Einbau zusätzlicher Komponenten
- Testen der gesamten Konfiguration (Risikoausschluss: Dead on Arrival)
- Installation des PBeaKK Standard Images
- Installation zusätzlicher Software gemäß Arbeitsanweisung
- Pflege der relevanten Asset-Information (z.B. Mac-Adresse, Serien-Nummer) gemäß Vorgabe der AG im Asset Management System
- Eintrag des BIOS-Passworts
- Dokumentation nach Vorgabe der AG

Inbetriebnahme von Clients

Folgende Leistungen sind zu erbringen

- Terminvereinbarung mit dem Endkunden
- Transport und Auslieferung der Ware an den Endkunden.
- Anschluss und Inbetriebnahme der Geräte und der mitbestellten Zusatz-HW wie z.B. Bildschirm oder Portreplicator (inkl. Einstellung der notwendigen Parameter) gemäß Vorgabe der AG
- Durchführung eines Funktionstests vor der Auslieferung
- Bei Ersatzbeschaffung: Datenübertragung der relevanten Festplatteninformation auf das Neugerät. Dazu werden die Daten auf einem speziellen Netzlaufwerkverzeichnis vom Kunden vorab gesichert
- Anbringen der Geräteidentifikation gemäß Vorgaben des AG
- Kurzeinweisung des Kunden in die wesentlichen Bedienpunkte der neuen HW
- Übernahmeformular ausfüllen, von Kunden unterschreiben lassen und archivieren
- Mitnahme und Entsorgung Verpackungsmaterial nach geltenden Umweltschutz-Vorschriften

10.1.2 Außerbetriebnahme von Clients

Hardware

Abbau bzw. Verschrottung von bestehender Hardware (Clients, Zubehör, Software und Peripherie gem. HW/SW-Warenkorb) nach Vorgabe der AG.

Folgende Leistungen sind zu erbringen:

- Terminplanung bei Einzelumfängen:
- Terminvereinbarung mit dem Endkunden
- Abbau, Abholung des Alt-PC / Hardware vor Ort nach Vorgabe des AG
- Bei Systemen mit HDDs: Lokale Daten vor Rücktransport löschen (nach Gutmann-Verfahren oder adäquates Verfahren)
- Abtransport und Übergabe der Alt Hardware an zentrale Stelle nach Vorgabe des AG
- Dokumentation der Gerätedaten (Deaktivierung Altgerät/Anlage Neugerät) durch AN

Software

- Deinstallation der Software gemäß Vorgaben der AG
- Ziel ist in jedem Fall Erhalt und Weitergabe von ggf. vorhandenen Lizenzschlüsseln

10.2 Softwarepaketierung

Die Paketierung/Aktualisierung der Software im Standardwarenkorb ist im Betriebspreis der Clients enthalten. Für den Fall, dass die AG zusätzliche Paketierungsleistungen benötigt, werden u.a. folgende Leistungen (Auszug) erforderlich:

- Analyse des Auftrages hinsichtlich technischer Machbarkeit und Termin/Aufwand
- Entwicklung/Paketierung
- Test der Anwendung, laborintern und auf benannten Clients der AG in Abstimmung mit dem AG, incl. Abnahme durch die AG
- Durchführung von Performancetests auf Referenzclients (z.B. Laden des Profils)
- Produktfreigabe

Diese Leistungen werden auf Basis von T&M erbracht.

11 Hinweise zur Bepreisung der Leistungen

Die Vergütung erfolgt auf Basis eines monatlichen Pauschalpreises je verwaltetem Client (Mietgeräte inklusive Managed Service), getrennt nach HW-Miete und Service. Der Preis ist abhängig von der gewählten Geräteklasse.

Die monatlichen Pauschalen decken die Hardware-Miete und alle beschriebenen Managed-Service-Leistungen ab. Leistungen über die beschriebenen hinaus sowie erweiterte Projektleistungen (Rollouts, Migrationen, Sondersoftware-Paketierung) werden nach Aufwand auf Basis der aktuellen Preisliste des Auftragnehmers berechnet. Dazu zählen auch die Erstellung bzw. die Aktualisierung von zusätzlichen Softwarepaketen.

Die Angaben über Mengengerüste und allgemeine Hinweise zu den Pauschalen dienen zur Unterstützung der Kalkulation des Angebotes. Die AG weist ausdrücklich darauf hin, dass die genannten Zahlen der Veränderung unterliegen können und Abweichungen von +/- 10% keine preislichen Auswirkungen haben.

Die Leistungen werden weitgehend von Montag – Freitag 08:00 – 17:00 Uhr erbracht. In Ausnahmefällen und bei besonderen Tätigkeiten (z.B. Migrationen, Updates) müssen diese Leistungen auch außerhalb dieser Zeiträume erbracht werden.

Die AG strebt für die Leistungen des Vertrages ein möglichst einfaches, aber in jedem Fall nachvollziehbares Preismodell an.

Die Bepreisung ist ausschließlich im Preisblatt „Managed Client 2027“ vorzunehmen.

11.1 Standardleistungen

Die Standardleistungen fließen mit jeweils 100% in den Gesamtpreis ein. Hardware und Betriebspauschalen werden ab dem 01.04.2027 fällig.

11.2 Optionale Leistungen

Die optionalen Leistungen fließen mit jeweils 50% in den Gesamtpreis ein.

Die Tagessätze für die Unterstützungsleistungen sind auf der Basis 8h inkl. ggf. anfallender Reise- und Nebenkosten abschließend anzugeben.

Das Mengengerüst für die optionalen Leistungen basiert auf Schätzungen der AG für den Bedarf während des maximalen Leistungszeitraumes von 36 Monaten.

12 Anhänge

- Anhang 1: Leistungsverzeichnis Hardware (LV-Hardware) mit technischen Spezifikationen je Gerätekategorie
- Anhang 2: Standard-Softwarekorb
- Anhang 3: Übersicht der anzupassenden BIOS-Einstellungen

12.1 Leistungsverzeichnis Hardware (LV-Hardware) mit technischen Spezifikationen je Gerätekategorie

Mengengerüste

Gerätekategorie	Geschätzte Anzahl	Poolgeräte zusätzlich
Desktop Performance	10	0
Laptop Standard	400	10
Laptop Performance	20	0
Docking Station	505	5
Mobiltelefon Standard	150	5
Mobiltelefon Erweitert	20	0
Tablet Standard	20	0

Jeder Laptop wird mit einer Docking Station auszustatten, die den Anschluss von zwei zusätzlichen Bildschirmen (27 Zoll) über Display Port erlaubt. Zusätzlich werden weitere 75 Docking Stationen in den Liegenschaften der Auftraggeberin bereitgestellt. Die Docking Stations müssen über einen Ein-/Ausschalter für die Laptops verfügen.

Technische Anforderungen an die Geräte

Nachfolgend sind die Mindestanforderungen an Leistung, Akku, Bildschirmgröße, Mobilfunk beschrieben.

Modell	Betriebssystem	Leistung	Akku	Bildschirmgröße	Sonderausstattung
Desktop Performance	Windows 11	CPU 16 Kerne Turbo-Boost Takt mind. 5.5GHz für P-Cores, 32 GB RAM, 1 TB SSD	-/-	-/-	Dedizierte GPU (z.B. NVIDIA RTX 3050 oder neuer/besser)

Laptop Standard	Windows 11	CPU 6 Kerne Turbo-Boost Takt mind. 4.4GHz für P-Cores, 16 GB RAM, 512 GB SSD	Laufzeit Akku 8 Stunden	14 Zoll	
Laptop Performance	Windows 11	CPU 16 Kerne Turbo-Boost Takt mind. 5.3GHz für P-Cores, 32 GB RAM, 1 TB SSD	Laufzeit Akku 6 Stunden	15.6 Zoll	Dedizierte GPU z.B. (NVI- DIA RTX 3050 oder neuer/besser)
Mobiltelefon Standard	iOS	A19, 8 GB RAM, 256 GB Speicher	Laufzeit Akku 27 Stunden	6.3 Zoll	5G, Face-ID, 48 MP Kamera
Mobiltelefon Erweitert	iOS	A19 Pro, 12 GB RAM, 256 GB Speicher	Laufzeit Akku 33 Stunden	6.9 Zoll	5G, Face-ID, 48 MP Kamera, Telefoto
Tablet Standard	padOS	Apple M4, 12 GB RAM, 256 GB Speicher	Laufzeit Akku 9 Stunden	13 Zoll	Apple Pencil Support, Face- ID, 4G/5G

Für die Desktop-Geräte sind zusätzlich folgende Ausstattungen vorzusehen:

- TPM 2.0
- Secure Boot
- SSD
- USB A/C
- Bluetooth
- 2x Display Port

Für die Laptop-Geräte sind zusätzlich folgende Ausstattungen vorzusehen:

- Integrierte Webcam
- USB-C
- WLAN 6
- Fingerprint-Sensor
- TPM 2.0
- Secure Boot

Für die Mobiltelefone und die Tablets werden folgende Ausstattungsmerkmale gefordert:

- 5G
- Face-ID

12.2 Standard-Softwarekorb

Nr	Software Paket
1	1.01.01.000_Adobe_Reader
2	1.03.00.000_PBeaKK_WerBinIch
3	1.04.00.000_Cisco_SecureClient
4	1.05.01.001_Citrix_Workspace
5	1.07.00.000_DonHo_Notepad++
6	1.11.00.000_Caseris_CaesarConnector
7	1.13.00.000_IgorPavlov_7-Zip
8	1.02.00.000_Oracle_Java_1.8
9	2.20.00.000_GreenshotTeam_Greenshot
10	2.01.02.000_Adobe_AcrobatPro
11	1.00.00.000_Microsoft_OfficeStandard_2024
12	2.31.00.000_ControlUp_ControlUpAgent
13	1.06.01.001_WebEx

12.3 Übersicht der anzupassenden BIOS-Einstellungen

Option	Wert	Kommentare
Bios Kennwort	gesetzt	Der AG definiert das Kennwort
TPM 2.0	dTPM, Hardware Chip	kein fTPM
Virtualisierung	aktiv	
Secure Boot	aktiv	mit den neuesten UEFI-Zertifikaten
Boot Reihenfolge	fest	definiert durch AG
Boot Menu Taste	aktiv	z.B. F12

Option	Wert	Kommentare
Wake on Lan	aktiv	
IPv6 PXE Boot	deaktiviert	
MAC Address Passthrough	aktiv	Internal MAC weitergeleitet an Docking Station
Always ON USB	aktiv	
Firmware Update	aktiv	via OS-Update
Boot Order Lock	inaktiv	