Leistungsbeschreibung

Bereitstellung von Arbeitsplatzlösungen

der

BARMER

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Der *Auftraggeber* BARMER (im folgenden auch *Auftraggeber*) gehört zu den führenden gesetzlichen Krankenkassen in Deutschland. Die Versicherten des *Auftraggebers* profitieren von hervorragenden Leistungen, einer erstklassigen medizinischen Versorgung und einem breit aufgestellten Gesundheitsnetzwerk.

Die besondere Leistungsstärke des *Auftraggebers* wird regelmäßig in Krankenkassen-Vergleichen bestätigt. Weitere Informationen finden Sie unter www.barmer.de.

Im Text wird aus Gründen der Lesbarkeit auf eine geschlechtergerechte Formulierung verzichtet. Es sind jedoch immer alle Geschlechter angesprochen.

2 Übersicht über die im Rahmen der IT-Modernisierung geplanten Ausschreibungen

Die BARMER und die HEK führen im Zusammenhang mit der Modernisierung teilweise gemeinsame Beschaffungen durch. Ein Überblick über diese Ausschreibungen findet sich in diesem Kapitel weiter unten. Die vorliegende Ausschreibung “Bereitstellung von Arbeitsplatzlösungen” ist ausschließlich eine Beschaffung der BARMER, d.h. die HEK ist nicht Auftraggeber dieses Vergabeverfahrens.

Das vorliegende Vergabeverfahren betrifft ein IT-Modernisierungsprojekt des *Auftraggebers*. Die folgenden Kapitel sollen potenziellen Anbietern einen Überblick über die aktuell geplanten Vorhaben, Erwartungen und Ausschreibungen des *Auftraggebers* geben, die für ein übergreifendes Verständnis des Bieters zum aktuellen Vergabeverfahren von Bedeutung sind.

Der *Auftraggeber* plant eine umfassende Modernisierung seiner bestehenden IT-Infrastruktur, welche zurzeit durch aktuelle Dienstleister bereitgestellt und betrieben wird.

Die Modernisierung beinhaltet im engeren Sinne (Kernausschreibungen) die Neuvergabe von folgenden Themen:

- Bereitstellung und Betrieb von **SAP** (Ausschreibung TZB-SAP-2025)
- Bereitstellung und Betrieb von **Enterprise Core** (Ausschreibung TZB-EC-2025)
- Bereitstellung und Betrieb von **Arbeitsplatz** Lösungen (Ausschreibungen TZB-AP-2025 – nur für den *Auftraggeber* BARMER).

Des Weiteren sind u.a. Ausschreibungen in den Bereichen Connectivity, IT-Security und IT Service Management Tool geplant. Die mit diesen Ausschreibungen zu beschaffenden Leistungen sind für die drei oben genannten Ausschreibungen (SAP, Enterprise Core und Arbeitsplatz) Beistellungen des *Auftraggebers* und haben direkte oder indirekte Abhängigkeiten zu diesen Ausschreibungen.

Der Bieter muss diese Abhängigkeiten in seinem Lösungsvorschlag in Architektur, Design, Implementierung, Test und der Transition/Transformation berücksichtigen (zu den diesbezüglichen Anforderungen siehe **00-05 Angebotswertung**).

In der nachfolgenden Übersicht sind die geplanten Ausschreibungen im Überblick dargestellt:

Ausschreibungen		
#	**Scope**	**Auftraggeber**
1	SAP Infrastruktur und Basis-Betriebsleistungen	BARMER und HEK
2	Enterprise Core	BARMER und HEK
3	**Arbeitsplatz**	**BARMER**
4	Data Center Connectivity and Network Services • DC-WAN Connectivity • Basis Netzwerkdienste (DDI)	BARMER
5	IT-Security • Managed SOC • Managed Connectivity Security • Security Audit Tools	BARMER
6	Identity Management (IDM) & Identity and Access Management (IAM), Privileged Access Management (PAM), PKI as a Service	BARMER
7	IT Service Management Tool (ServiceNow)	BARMER

Tabelle 1: Ausschreibungsübersicht

Für einen ersten Einblick werden im Folgenden kurz die voraussichtlichen Gegenstände der genannten Ausschreibungen skizziert: Diese haben gegebenenfalls Auswirkungen auf die Architektur, das Design und die Implementierung der Arbeitsplatz Services.

- Die Ausschreibung **SAP Managed Service** umfasst die Bereitstellung und den Betrieb der SAP-Systemumgebung des Auftraggebers. Ein wichtiger Bestandteil der Plattform ist das Versichertenbestands-, Beitrags- und Leistungs-Management, sowie weitere Fachprozesse, welche auf der SAP-basierten Branchen-Software oscare® aufsetzen.
- Die Ausschreibung für **Enterprise Core** umfasst die Bereitstellung zentraler IT-Services zur Unterstützung des IT-Betriebs und der digitalen Infrastruktur. Hierzu zählen auch das Input-, Output- und Archivmanagement, IT-Basisdienste sowie Intranet-Systeme. Weitere Aufgaben umfassen die Betreuung der Eigenentwicklungsplattform und der Testautomatisierung, den Betrieb von Data- und Analytics-Systemen, die Bereitstellung von Container- und Eventstreamingplattformen sowie die Verwaltung und den technischen Betrieb von Kaufsoftware.
- Die Ausschreibung **Arbeitsplatz** umfasst die Bereitstellung und den Betrieb von Lösungen für virtuelle und physische Arbeitsplätze, Drucker, Anwender-Software, Exchange-Betrieb und Software-Management.
- Die Ausschreibung **Data Center Connectivity and Network Services** umfasst die Netzwerkverbindung zwischen den drei „Data Centern“ (siehe Kapitel 4) und Netzwerkbasisdienste wie z.B. DNS, DHCP und IPAM und alle dafür erforderlichen Hard- und Softwarekomponenten sowie Services.
- Mit der Ausschreibung **IT-Security** plant der *Auftraggeber* eine neue IT-Sicherheitsarchitektur, z.B. die Erweiterung der detektiven Toollandschaft oder die Ausweitung der Zero-

Trust Strategie.

- Mit der Ausschreibung **Identity Management (IDM) & Identity and Access Management (IAM)** plant der *Auftraggeber* eine neue Identity und Access Management Lösung und die Einführung eines Privileged Access Managements.
- Mit der Ausschreibung **IT Service Management Tool (ServiceNow)** plant der *Auftraggeber* Lizenzen für die aktuell im Einsatz befindliche ITSM-Suite zu beschaffen. Des Weiteren ist eine Modernisierung und Erweiterung der bestehenden ITSM Prozesse geplant.

3 Grundsätzliche Anforderungen an die Leistungserbringung

Der *Auftraggeber* erwartet eine flexible Leistungserbringung, die sowohl das kurzfristige Hinzubuchen von IT-Produkten und Infrastruktur-Komponenten als auch das Anpassen von IT-Prozessen oder ganz allgemein die flexible Inanspruchnahme von IT-Leistungen ermöglicht. Dies umfasst auch die flexible Reduzierung von Leistungen. Die Sicherstellung der Flexibilität ist neben der Qualität, Verfügbarkeit und Performance ein wesentliches Ziel der Ausschreibungen.

Es lassen sich unter anderem folgende Ziele festhalten, deren Erreichung der *Auftragnehmer* jederzeit sicherzustellen hat:

- Flexibilität des *Auftraggebers* im Hinblick auf den Umfang der in Anspruch genommenen Leistungen
- Kurzfristige Erfüllung externer regulatorischer Anforderungen, z.B. zur Mitigation von Ergebnissen aus Audits oder Gesetzesänderungen
- Konzeption, Steuerung und Umsetzung einer reibungsarmen Transition
- Einhaltung der gesetzlichen Vorgaben sowie der besonderen Anforderungen des *Auftraggebers* zur Sicherstellung der IT-Compliance
- Einsatz innovativer und zukunftssicherer Technologien
- Alle IT-Services/-Systeme basieren auf aktueller (Stand der Technik) leistungsfähiger Hard- und Software
- Kontinuierliche Anpassung an die Erfordernisse des Geschäftsbetriebs des *Auftraggebers* und Optimierung der IT-Services/-Systeme und -Prozesse
- Bereitstellung von Read-only Accounts für die für den *Auftraggeber* bereitgestellten Systeme und Services

4 Bereitstellungsmodelle für „Data Center“

Der *Auftraggeber* unterscheidet zwei Bereitstellungsmodelle für das "Data Center": "Dedicated Ressources" (kurz "Dedicated") und "Shared Ressources" (kurz "Shared"). Der *Auftraggeber* will bei den angefragten Leistungen der Ausschreibungen “SAP” und “Arbeitsplatz” die Potenziale des Marktes ausschöpfen. Wie nachfolgend beschrieben, können die Bieter im Rahmen der Vergabeverfahren “SAP” und “Arbeitsplatz” daher entweder das Bereitstellungsmodell “Dedicated” **oder** das Bereitstellungsmodell “Shared” **oder** – im Wege der Abgabe von zwei Hauptangeboten – sowohl das Bereitstellungsmodell “Dedicated” **als auch** das Bereitstellungsmodell “Shared” anbieten. Im Rahmen der Auftragsausführung wird nur eines der beiden Bereitstellungsmodelle zur Anwendung kommen. Bei der Ausschreibung “Enterprise Core” ist nur das Bereitstellungsmodell “Dedicated” zugelassen.

Der *Auftraggeber* behält sich vor, im weiteren Verlauf des Vergabeverfahrens das Kombinationsverbot (siehe weiter unten) aufzuheben und ein Hybrid-Modell (d.h. eine Kombination aus „Dedicated“-Ansätzen und „Shared“-Ansätzen im gleichen Bereitstellungsmodell) zuzulassen. Hierzu wird im Einzelnen auf **00-01 Allgemeine Verfahrensbedingungen** Ziffer 6.1, verwiesen.

„Dedicated Resources“ – kurz „Dedicated“

In diesem Bereitstellungsmodell erfolgen die Bereitstellung und der Betrieb durch dedizierte Server-Infrastruktur in einem physikalisch isolierten Bereich als exklusive Ressource für den *Auftraggeber*.

„Shared Resources“ kurz „Shared“

In diesem Bereitstellungsmodell stellt der *Auftragnehmer* eine Infrastruktur bereit, die bedarfsorientiert von verschiedenen Kunden (Mandanten) des *Auftragnehmers* gemeinsam genutzt werden kann. Die Workloads (Services) des *Auftraggebers* sind dabei nicht physikalisch, wohl aber Software-technisch von anderen Kunden des *Auftragnehmers* getrennt.

Beide Bereitstellungsmodelle müssen darüber hinaus folgende Anforderungen erfüllen:

Der *Auftragnehmer* und von ihm zur Leistungserbringung eingesetzte Drittunternehmen haben bei der Verarbeitung von Sozial- und Gesundheitsdaten im Wege des Cloud-Computing-Dienstes die Vorgaben der § 393 Abs. 2 und 3 SGB zu beachten. Das bedeutet, dass die Verarbeitung nur 1. im Inland, 2. in der Region EU / EWR oder 3. in einem Drittstaat mit Angemessenheitsbeschluss erfolgen darf, sofern die datenverarbeitende Stelle über eine Niederlassung im Inland verfügt. Die Datenhaltung von Sozialdaten und Gesundheitsdaten darf ausnahmslos nur in der Region EU / EWR plus Schweiz erfolgen. D.h. der Serverstandort muss sich in der Region EU / EWR plus Schweiz befinden. Sollte das Geschäftsmodell des *Auftragnehmers* bzw. des von diesem eingesetzten Drittunternehmen im Rahmen eines “Follow-the-sun" Prinzips grundsätzlich auch Supportleistungen aus Drittstaaten ohne Angemessenheitsbeschluss beinhalten, so sorgt der *Auftragnehmer* dafür, dass dieser Support für den *Auftraggeber* unterbleibt. Klarstellend wird darauf hingewiesen, dass jeglicher Transfer von Sozialdaten und Gesundheitsdaten in andere Drittstaaten unzulässig ist.

Für die Ausschreibungen „SAP“, „Enterprise Core“ und „Arbeitsplatz“ dürfen durch die Bieter folgende Bereitstellungsmodelle angeboten werden:

#	Scope	Dedicated	Shared
1	SAP	Ja	Ja
2	Enterprise Core	Ja	Nein
3	Arbeitsplatz	Ja	Ja

Tabelle 2: Bereitstellungsmodelle

In den drei Ausschreibungen werden diverse Services angefragt. Die Bereitstellung der Services in einem Angebot muss durchgängig mit einem Bereitstellungsmodell, also entweder im Modell „Dedicated Resources“ oder im Modell „Shared Resources“ erfolgen. Die Bieter können jedoch zwei Hauptangebote abgeben, wenn sie sowohl „Dedicated“ als auch „Shared“ anbieten wollen.

Eine Kombination der Bereitstellungsmodelle in einem Angebot (z.B. für verschiedene Services im Rahmen eines Angebots) ist nicht zulässig. Beispiel: Diese Kombination ist NICHT zulässig:

#	Ausschreibung und Service	Dedicated	Shared
3	Arbeitsplatz | Service Virtueller Arbeitsplatz	Angebot	-
3	Arbeitsplatz | Service Arbeitsplatzdruck	-	Angebot

Tabelle 3: Ausschreibung und Service

5 Übersicht der Grob-Architektur im Zielbild

Der *Auftraggeber* möchte nicht ein reines Abbild der aktuellen Systemlandschaft neu beschaffen, vielmehr soll folgendes Zielbild (**Fehler! Verweisquelle konnte nicht gefunden werden.**) umgesetzt werden:

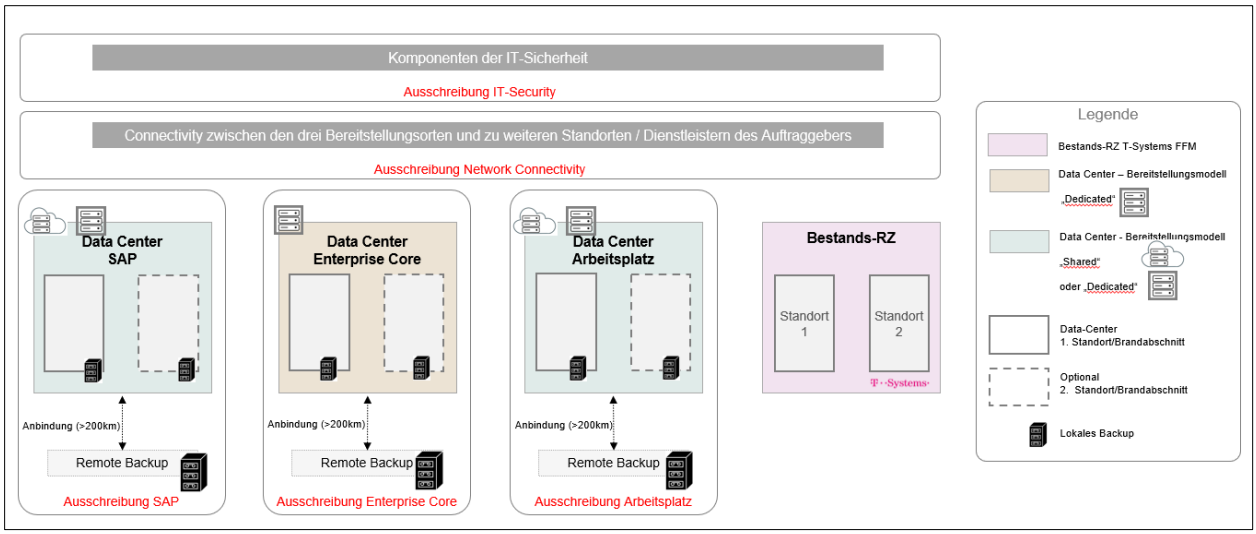

Abbildung 1: Grob-Architektur

Die Darstellung beschreibt die Verortung der geplanten Ausschreibungen auf einer Grob-Architektur und stellt kein finales Architekturbild da. Die Skizze enthält das Bestands-Rechenzentrum der T-Systems, welches in Frankfurt / Main angesiedelt ist. Vor dem Hintergrund der vorgenannten drei Neuausschreibungen ist denkbar, dass die jeweils ausgeschriebenen Services zukünftig aus bis zu drei unterschiedlichen “Data Centern” erbracht werden. Für die Transition wird das Bestands-Rechenzentrum mit den maximal drei weiteren „Data Centern“ (Data Center SAP, Data Center Enterprise Core, Data Center Arbeitsplatz) verbunden werden. Diese Netzwerkverbindung wird durch den *Auftraggeber* beigestellt.

6 Struktur der Leistungsbeschreibung und der zugehörigen Anlagen

Die Leistungsbeschreibung enthält eine Kurzbeschreibung der einzelnen Services, die der *Auftragnehmer* erbringen muss. Zur Festlegung und Definition der vom *Auftragnehmer* zu erbringenden Leistungen verwendet der *Auftraggeber* neben dieser Leistungsbeschreibung eine Reihe von weiteren ineinandergreifenden Dokumenten. Der folgende Abschnitt erläutert diese Struktur und gibt einen Überblick über die Dokumente, in denen die Leistungspflichten des *Auftragnehmers* hinterlegt sind.

Folgende Anlagen zur Leistungsbeschreibung werden im Rahmen dieser Ausschreibung für die Beschreibung der Leistung verwendet, auf deren Inhalt im Folgenden kurz eingegangen wird:

- **01-02 Leistungsbeschreibung**
- **01-02-01 Service Katalog**
- **01-03 Technologiedefinitionen**
- **01-04 Service Levels**
- **01-05 Berichte**
- **01-06 Leistungsverzeichnis**
- **01-07 Skillprofile**
- **01-08 Transition**

- **01-09 Assets**

6.1 Leistungsbeschreibung

Die Leistungsbeschreibung beinhaltet den Gegenstand der Beschaffung in Form einer Kurzbeschreibung der einzelnen Services, die der *Auftragnehmer* vollumfänglich und unter Berücksichtigung der übergreifenden Regelungen und Anforderungen erbringen wird. In der Leistungsbeschreibung wird für weitere Informationen zu den einzelnen Services auf die nachfolgenden Dokumente, insbesondere auf den **01-02-01 Service Katalog,** verwiesen. Zudem enthält sie einen Überblick über die Rahmenbedingungen für diese Ausschreibung.

6.2 Service Katalog

Im Service Katalog werden die einzelnen Services und deren Servicevarianten entsprechend den Anforderungen an die Leistungserbringung detailliert aufgeführt. Die Servicevarianten dienen dabei zur Unterscheidung von Anforderungen innerhalb eines Service. Dies können z.B. Servicezeiten, Verfügbarkeiten oder andere Parameter sein, für die in den jeweiligen Servicevarianten unterschiedliche Ausprägungen vorgegeben werden können.

Für jede Servicevariante ist im Service Katalog unter anderem festgelegt:

- Welche Service Level, Servicezeiten, Betriebszeiten und weitere Anforderungen an den Betrieb gelten.
- Welche Prozessrichtlinien, deren Ergebnisse, Hindernisse und Mitwirkungspflichten durch den Auftragnehmer entsprechend **02-04 Prozessrichtlinien** zu berücksichtigen sind.
- Welche Vergütungseinheit je Servicevariante Anwendung findet.

Weitere Erläuterungen sind dem Servicekatalog im Arbeitsblatt *Einführung* zu entnehmen.

6.3 Technologiedefinitionen

In den Technologiedefinitionen werden servicespezifische und technische Anforderungen und Details (z.B. für bestehende Lösungen und Technologien) detaillierter erläutert, welche der *Auftragnehmer* für seine technische Lösung berücksichtigen muss. Diese Anforderungen und Details können aus Gründen der Lesbarkeit und Nachvollziehbarkeit nicht immer von der Beschreibung der Anforderung an den Leistungsgegenstand abgegrenzt werden. Daher sind für die einzelnen Services immer die entsprechenden Passagen in der Leistungsbeschreibung und in den Technologiedefinitionen im Zusammenhang zu sehen.

6.4 Service Levels

Bei der Erbringung der Leistung hat der *Auftragnehmer* die festgelegten SLA´s einzuhalten. Diese sind in der Anlage **01-04 Service Levels** beschrieben und spezifiziert. Darüber hinaus sind dort Festlegungen u.a. zu den Service Level Klassen und Service Zeiten hinterlegt.

6.5 Berichte

Die Anforderungen an das Reporting (Art, Umfang, Inhalt, Frequenz etc.) sind in der Anlage **01-05 Berichte** definiert und durch den *Auftragnehmer* entsprechend einzuhalten.

6.6 Leistungsverzeichnis

Im **01-06 Leistungsverzeichnis** werden für die einzelnen Services und Servicevarianten die jeweiligen Preise hinterlegt, die während der Vertragsumsetzung zur Abrechnung kommen. Dabei wird immer auf eine eindeutige Servicevariante referenziert. Allgemeine Festlegungen zu den Vergütungsmodellen und spezifische Erläuterungen zum Leistungsverzeichnis finden sich in der

Anlage **02-08 Vergütung**.

6.7 Skillprofile

Insbesondere zur Durchführung von Projekten und zur Erbringung von Beratungsleistungen, z.B. für die technologische und strategische Weiterentwicklung, muss der *Auftragnehmer* Mitarbeiter mit entsprechenden Skillprofilen bereitstellen. Die Anforderungen an die Skillprofile sind in der Anlage **01-07 Skillprofile** beschrieben.

6.8 Transition

Zum Aufbau der benötigten Systeme und zur Übernahme der geforderten Services erbringt der *Auftragnehmer* Transitionsleistungen, die in der Anlage **01-08 Transition** beschrieben sind. Die Transition erfolgt auf Grundlage des von dem *Auftragnehmer* eingereichten Transitionskonzepts (**01-08-01 Transitionskonzept**) nebst Anlagen (**01-08-01-01 Transition Zeitplan**, **01-08-01-02 Transition Risiken**, **01-08-01-03 Transition Auftraggeber Ressourcen**).

6.9 Assets

Der *Auftraggeber* bringt in das Vertragsverhältnis Lizenzen, Verträge, Tools und sonstige Assets mit ein, die in der Anlage **01-09 Assets** hinterlegt sind. Diese Assets müssen bei der Angebotserstellung berücksichtigt werden und dürfen nicht zusätzlich angeboten und berechnet werden.

6.10 Übergreifende Anforderungen

Im Rahmen dieser Leistungsbeschreibung werden neben den spezifischen Anforderungen auch übergreifende Regelungen berücksichtigt, die grundlegende Anforderungen enthalten. Auf diese übergreifenden Regelungen wird an verschiedenen Stellen Bezug genommen. Es wird vorausgesetzt, dass der *Auftragnehmer* die Inhalte dieser Regelungen kennt und diese entsprechend einhält.

Der *Auftragnehmer*:

- hält sich an die allgemeinen Bestimmungen zu IT-Dienstleistungen und Lösungen, die in der Anlage **02-02 Technologiegrundsätze** beschrieben sind.
- beteiligt sich an der in der Anlage **02-03 Governance** fixierten Governancestruktur und den damit zusammenhängenden Prozessen.
- erbringt in Verbindung mit den hier beschriebenen Services die in der Anlage **02-04 Prozessrichtlinien** beschriebenen funktionsübergreifenden Dienste.
- hält bei der Erbringung von projektbezogenen Leistungen die in der Anlage **02-05 Projektgrundsätze** hinterlegten Anforderungen ein.
- berücksichtigt die in der Anlage **02-06 Beendigungsgrundsätze** hinterlegten Anforderungen an das Beendigungsmanagement bei Vertragsende im Rahmen der geschlossenen Vertragsbeziehung.
- kennt und berücksichtigt die in der Anlage **02-07 Leistungssteuerungsgrundsätze** hinterlegten Regelungen für die Steuerung der Vertragsleistungen, insbesondere mittels Service Leveln.
- berücksichtigt bei der Berechnung der Vergütung für die Erbringung der Leistungen die Festlegungen in der Anlage **02-08 Vergütung**.

- hält die Vorgaben des *Auftraggebers* in Bezug auf Datenschutz und Informationssicherheit ein, die in den Auftraggeberrichtlinien, insbesondere in den Anlagen **02-09-02 Auftragsverarbeitungsvereinbarung** und **02-09-03 AVV TOMs Informationssicherheit,** hinterlegt sind.
- muss für alle KRTIS-relevanten Services dauerhaft sicherstellen, dass die in **02-09-03 AVV-TOMS Informationssicherheit** beschriebenen KRITIS-Regularien angewandt und erbracht werden. Als KRITIS-relevant gelten alle Services in **01-02 Servicekatalog**, die entsprechend gekennzeichnet sind. KRITIS-Regularien können sich während der Vertragslaufzeit ändern (bspw. aufgrund von Gesetzesänderungen oder Änderungen beim *Auftraggeber*) und werden dem *Auftragnehmer* vom *Auftraggeber* bekanntgegeben.

7 Gegenstand der Beschaffung

Die Anforderungen an IT-Arbeitsplatzlösungen unterliegen einem stetigen Wandel, getrieben durch technologische Innovationen, zunehmende Mobilität der BARMER Belegschaft und den steigenden Bedarf an nahtloser Zusammenarbeit in einer vernetzten Arbeitswelt.

Der Arbeitsplatz des *Auftraggebers* muss nicht nur den individuellen Anforderungen der Nutzer gerecht werden, sondern auch flexibel und sicher gestaltet sein, um den sich ständig verändernden Rahmenbedingungen des *Auftraggebers* Rechnung zu tragen.

In diesem Zusammenhang ist ein effizient und effektiv gestaltetes Infrastruktur-Sourcing ein entscheidender Faktor, um den Betrieb stabil, skalierbar und zukunftssicher zu gestalten.

Die vorliegende Ausschreibung beschreibt die Anforderungen und Leistungen im Bereich der Arbeitsplatz Services, die als integraler Bestandteil der IT-Infrastruktur eine optimale Arbeitsumgebung für alle Nutzer sicherstellen sollen.

7.1 Zusammenfassung der Arbeitsplatz Managed Services

Die Arbeitsplatz Managed Services (inkl. grundlegender Infrastruktur Services & Netzwerkbasisleistungen) lässt sich in zwei Servicegruppen aufteilen: Arbeitsplatz Services und Kommunikation & Kollaboration.

Die **Arbeitsplatz Services** umfassen folgende Services:

- **Virtueller Arbeitsplatz:**
  - Bereitstellung und Betrieb von virtuellen Arbeitsplätzen mittels einer Virtual Desktop Infrastructure (VDI).
  - Bereitstellung einer virtuellen Umgebung auf Basis des jeweils aktuellen Windows Betriebssystems, das alle Standardfunktionen von Windows unterstützt.
- **Office Arbeitsplatz:**
  - Integrierte und optimierte Arbeitsumgebung für klassische Fat-Clients mit Microsoft Windows.
  - Bereitstellung, Betrieb, Verwaltung und kontinuierliche Optimierung der Arbeitsplatzumgebung, Betriebssysteme und Anwendungen.
- **Software-Management:**
  - Bereitstellung, Verwaltung und Wartung der beim *Auftraggeber* im Einsatz eingesetzten Softwarekomponenten auf allen Managed-Clients (Fat-Clients und VDIs).

- Automatisierte Bereitstellung von Betriebssystemen, Virtualisierungslösungen sowie paketierter Software.

- **Arbeitsplatz Druck:**
  - Bereitstellung und Management von Konfigurationen für Multifunktionsdrucker und Druckservern.
  - Bereitstellen einer Lösung für die Selbstverwaltung von Multifunktionsdruckern (Druck-Self-Service-Portal).

Innerhalb **Kommunikation & Kollaboration** sind das Bereitstellen und Betreiben einer ganzheitlichen Kommunikations- und Kollaborationsinfrastruktur zur internen und externen Zusammenarbeit Gegenstand dieser Ausschreibung. Im Einzelnen umfasst dies die folgenden Service Varianten:

- **File Services:**
  - Bereitstellung der Ressourcen für Fileshares.
- **E-Mail Services:**
  - Konfiguration und Betrieb der bestehenden On-Premises Infrastruktur, der Hybridkonfiguration sowie auch der Exchange Online Instanz.

Die Zusammenarbeit mit dem neuen *Auftragnehmer* soll nicht nur die operativen Anforderungen des laufenden Betriebs sicherstellen, sondern auch eine Grundlage für die konstante Weiterentwicklung der IT-Infrastruktur schaffen. Dies beinhaltet insbesondere die Unterstützung bzw. Einführung neuer technologischer Trends sowie die kontinuierliche Weiterentwicklung der IT-Infrastruktur. Der *Auftragnehmer* muss die Anforderungen an die IT-Sicherheit, den Datenschutz sowie die Regulatorik (siehe **02-09-03 AVV TOMs Informationssicherheit**) einhalten und sicherstellen.

7.2 Technologische Beratungsleistungen zur Weiterentwicklung der Arbeitsplatz Services

Der *Auftragnehmer* berät den *Auftraggeber* aktiv bei der strategischen Weiterentwicklung der Arbeitsplatz Services sowie bei technologischen Modernisierungen. Die Beratungsleistungen sind Bestandteil des Leistungsumfangs und umfassen:

- Analyse und Bewertung von neuen Technologien, die für den *Auftraggeber* von Nutzen sein könnten
- Beratung bei der Gestaltung der IT-Architektur und des IT-Designs
- Beratung bezüglich des Einsatzes und der Integration neuer Technologien
- Initiale Entwicklung und kontinuierliche Weiterentwicklung der strategischen Roadmap zur Weiterentwicklung der Arbeitsplatz Services

Davon abzugrenzen sind konkrete Projektinitiativen, die beispielsweise aus den oben beschriebenen Beratungsleistungen resultieren können. Die Projektmitwirkung durch den *Auftragnehmer* wird in diesem Fall entsprechend der vereinbarten Skillprofile vergütet.

7.3 Kontinuierliche Verbesserung

Der *Auftragnehmer* ist für die kontinuierliche Verbesserung aller ausgeschriebenen Services verantwortlich. (Siehe **02-04 Prozessrichtlinien**)

7.4 Unterstützung bei Projekten

Der *Auftragnehmer* unterstützt den *Auftraggeber* bei der Durchführung von Projekten, die über

den im Service Katalog definierten Leistungsumfang sowie die Leistungsbestandteile der Transition hinausgehen.

Zur Umsetzung der Projekte wird der *Auftraggeber* vom *Auftragnehmer* unterschiedliche Skillprofile (siehe Anhang **01-07 Skillprofile** und Ziff. 10 dieser Leistungsbeschreibung) abrufen. Die Projekte nehmen Bezug auf die Weiterentwicklung der ausgeschriebenen Arbeitsplatz Services. Die Unterstützungsleistungen im Rahmen von Projekten können folgende Inhalte umfassen (nicht abschließend):

- Unterstützung bei der Integration neuer Technologien (bspw. Intune)
- Unterstützung bei der Migration von Services in Cloud Umgebungen
- Konfiguration und der Durchführung von Softwarerollouts,
- Unterstützung bei einem möglichen Wechsel der Telefonie Software (z.B. Webex durch Microsoft Teams)
- Unterstützung bei der Planung und Umsetzung von Architektur- und Designanpassungen

8 Schnittstellen und Integration

Die Integration in die IT-Landschaft des *Auftraggebers* sowie die Nutzung bewährter Schnittstellen sind entscheidende Faktoren für den reibungslosen Betrieb der virtuellen Arbeitsplätze. Die Lösung gewährleistet eine nahtlose Anbindung und erleichtert die Verwaltung sowie die Interaktion mit bestehenden Systemen.

Die Lösung ist so zu gestalten, dass sie nahtlos in die IT-Infrastruktur des *Auftraggebers*, unter Berücksichtigung aller Anforderungen aus dieser Leistungsbeschreibung und aus der Anlage **02-02 Technologiegrundsätze**, integriert werden kann. Dies umfasst u.a.:

- **Kompatibilität mit vorhandenen Netzwerken und Servern**: Einbindung in bestehende Netzwerkumgebungen ohne größere Anpassungen der bestehenden IT-Infrastruktur.
- **Infrastrukturdienste**: Verwendung der bestehenden Infrastrukturdienste des *Auftraggebers*
    - Administrationseinheit (OU)
    - Benutzerverwaltung
    - Domain Name System (DNS) - Intern & Extern
    - Domain Name System Security Extensions (DNSSEC)
    - DHCP
    - Roaming Profile
    - Forrest Roots
    - Authentifizierung/Zugriffssteuerung
    - IP-Adress Management (IPAM)
    - (Web-)Proxy-Server
- **Anwendungs-Integration**: Sicherstellung, dass die Systeme und Anwendungen (SAP, Genesys, etc.) in die virtuelle Umgebung eingebunden sind und mit der in den Service-Level Beschreibungen angeforderten Performance arbeiten und durch die Hersteller oder Dritte supported werden.
- **Integration mit bestehendem ITSM-Tool** (ServiceNow), wie in **02-02 Technologiegrundsätze** beschrieben.

8.1 Sicherheit der Daten

Grundlegende Anforderungen an die Sicherheit der Daten sind in der Anlage **02-09-03 AVV**

TOMs Informationssicherheit sowie der Anlage **02-02 Technologiegrundsätze** spezifiziert.

9 Grundlegende IT-Infrastruktur Leistungen

Unabhängig vom Bereitstellungsmodell (siehe Kapitel 4) sind die nachfolgenden Anforderungen vom *Auftragnehmer* einzuhalten.

Im Rahmen des Betreibermodells des *Auftragnehmers* sind alle Leistungen abzudecken, damit die IT-Infrastruktur ohne notwendige Zusatzleistungen, Support oder Lizenzen durch den *Auftraggeber* (oder von ihm beauftragten Dritten) verwendet werden kann. Davon ausgenommen sind Leistungen, welche im Service Katalog ausgeschlossen sind.

Im Folgenden sind grundlegende IT-Infrastruktur Leistungen, die für die Bereitstellung der Arbeitsplatz Services erforderlich sind, zusammengefasst. Der *Auftragnehmer* stellt sicher, dass die unten genannten Vorgaben ergänzend der Anlage **02-02 Technologiegrundsätze** eingehalten werden.

9.1 Kollaboration und übergreifende Steuerung

Die Aufgabe des *Auftragnehmers* ist es, einen stabilen und performanceoptimierten Betrieb der Systeme des *Auftraggebers* sicherzustellen und die Kooperation zwischen den Beteiligten, die in die Bereitstellung und den Betrieb der IT-Services eingebunden sind (unter anderem *Auftraggeber*, Dienstleister für Enterprise Core, Netzwerk, Security und User Helpdesk, sowie Bestandsprovider, AOK Systems, SAP und Querschnittsfunktionen des *Auftraggebers*), bestmöglich zu unterstützen.

9.2 Rechenzentrums-Leistungen

Ungeachtet des Bereitstellungsmodells (siehe Kapitel 4) muss der *Auftragnehmer* sicherstellen, dass eine geeignete Rechenzentrumsfläche und -infrastruktur in einem Rechenzentrum bereitgestellt wird. Dies umfasst beispielsweise die bedarfsgerechte Überwachung und Wartung der Hardware, Rack Housing, Klimatisierung, Zugangsschutz und eine geeignete Strom- und Netzanbindung der Leistungserbringungsorte des *Auftragnehmers*.

9.3 Datensicherung und Wiederherstellungs-Leistungen

Der *Auftragnehmer* ist verpflichtet, geeignete Maßnahmen zur Sicherung und Wiederherstellung aller Services zu ergreifen, um potenziellen Datenverlust und Ausfallzeiten zu minimieren. Hierzu sind Datensicherungen in einer Frequenz zu erstellen, die den Anforderungen der jeweils definierten Disaster-Recovery-Klassen in **01-04 Service Levels** und **01-03 Technologiedefinitionen** entspricht. Die Sicherungen sind auf hinreichend geschützten, verschlüsselten Speichermedien aufzubewahren.

Sofern der *Auftragnehmer* dem *Auftraggeber* Leistungen auf Basis von Shared-Technologien bereitstellt, sind sämtliche in diesem Dokument beschriebenen Anforderungen an Datensicherung und Wiederherstellung gleichermaßen zu erfüllen. Eine Abweichung hiervon bedarf der ausdrücklichen schriftlichen Zustimmung des *Auftraggebers*.

Leistungen Dritter, die im Auftrag des *Auftraggebers* im Rahmen von Housing- oder Hosting-Vereinbarungen erbracht werden, müssen in die vom *Auftragnehmer* bereitgestellte Backup- und Recovery-Infrastruktur integrierbar sein. Der *Auftragnehmer* hat hierfür entsprechende Schnittstellen und Prozesse bereitzustellen.

Im Rahmen der Transition ist der *Auftragnehmer* verpflichtet, ein dem Stand der Technik entspre-

chendes Datensicherungs- und Recovery-Konzept zu erstellen, dieses mit dem *Auftraggeber* abzustimmen, zu implementieren und während der gesamten Vertragslaufzeit fortlaufend zu betreiben und bei Bedarf anzupassen.

Folgende Mindestanforderungen gelten – in Abhängigkeit der jeweils vereinbarten Disaster-Recovery-Klasse (**01-02-01 Service Katalog** und **01-04 Service Levels**) – als Bestandteil der Backup- und Recovery-Architektur:

- Innerhalb des Data Center Verbundes (Datacenter 1. und 2. Standort, Abbildung 1: Grob-Architektur) ist eine lokale Backup- und Recovery-Infrastruktur bereitzustellen und durchgehend zu betreiben. Diese dient der kurzfristigen Störungsbehebung sowie der Erbringung sonstiger im Betrieb erforderlicher Leistungen.
- Zusätzlich ist an einem räumlich getrennten Standort eine redundante Backup- und Recovery-Infrastruktur zu betreiben. Der Mindestabstand zwischen dem Data Center Verbund (Datacenter 1. und 2. Standort, siehe Abbildung 1: Grob-Architektur), welcher im Rahmen dieser Ausschreibung angeboten wird, und dem Remote-Backup hat mindestens 200 km zu betragen. Diese Infrastruktur dient insbesondere der Notfallbewältigung im Sinne eines IT-Katastrophenszenarios sowie der Einhaltung gesetzlicher Vorgaben, insbesondere bei KRITIS-relevanten Systemen.
- Der *Auftragnehmer* stellt sicher, dass das Remote Backup mit Medienwechsel und unveränderlich durchgeführt wird (z.B. Tape).

Der *Auftragnehmer* ist berechtigt und aufgefordert, eigenständige und sinnvolle Anpassungen der Datensicherungsprozesse vorzunehmen, solange die vereinbarten Wiederherstellungsklassen und Verfügbarkeitsziele uneingeschränkt gewährleistet bleiben.

Die Durchführung und Frequenz von Datensicherungs-Zyklen sind mit dem *Auftraggeber* abzustimmen. Es ist sicherzustellen, dass eine Wiederherstellung auch versehentlich gelöschter Daten durch den *Auftraggeber* jederzeit möglich ist.

Der *Auftragnehmer* führt jährliche Desaster Recovery Übungen durch, um die Wirksamkeit der Wiederherstellungsprozesse zu testen und zu optimieren. Bei der Übung darf es zu keinen Ausfallzeiten für den *Auftraggeber* kommen.

Zugehörige Services in 01-02-01 Servicekatalog	
Zugehörige Service(s)	Alle relevanten Services entsprechend **01-02-01 Servicekatalog**
Zugehörige Service-ID(s)	Alle relevanten Service-ID(s) entsprechend **01-02-01 Servicekatalog**
Zugehörige Abrechnungseinheit(en) im Leistungsverzeichnis	Der *Auftragnehmer* berücksichtigt seine Aufwände und Kosten für Backup und Wiederherstellungs-Leistungen in den Services, in denen entsprechend **01-02-01 Servicekatalog** Grundlegende IT-Infrastrukturleisten zu berücksichtigen sind.

Tabelle 4: Services im Servicekatalog

9.4 Patch- und Update-Management-Leistungen

Der *Auftragnehmer* installiert Sicherheitsupdates und Patches für die Betriebssysteme und andere eingesetzten IT-Infrastrukturkomponenten einschließlich Firmware / BIOS-Update und testet die korrekte Funktionsweise, um die Sicherheit und Stabilität der Systeme zu gewährleisten.

Der *Auftragnehmer* erstellt in Abstimmung mit anderen ggf. betroffenen Dienstleistern des *Auftraggebers* einen konsolidierten Monatsplan, der alle geplanten Patch- und Updatemaßnahmen enthält. Er legt dem *Auftraggeber* den Monatsplan mit einer Vorlaufzeit von 4 Wochen zum Monatsbeginn vor. Der *Auftraggeber* gibt den vorabgestimmten Monatsplan schriftlich frei. Wird der Monatsplan aufgrund von zum Beispiel Qualitätsmängeln nicht durch den *Auftraggeber* freigegeben, so bessert der *Auftragnehmer* so lange nach, bis eine Freigabe erfolgen kann.

9.5 Storage-Leistungen

Der *Auftragnehmer* stellt Storage-Leistungen im Rahmen des Managed Services zur Verfügung. Diese Leistungen umfassen die Bereitstellung und Verwaltung von Speicherlösungen, die eine hohe Verfügbarkeit und Skalierbarkeit gewährleisten. Der *Auftragnehmer* sorgt für die Implementierung und Wartung von Storage Systemen. Regelmäßige Überprüfungen und Optimierungen der Speicherkapazitäten, Speicherinfrastruktur werden durchgeführt, um die Leistungsfähigkeit und Ausfallsicherheit zu maximieren.

Sollte durch den *Auftragnehmer* eine Bereitstellung mit Shared-Dienstleistungen angeboten werden, so muss der *Auftragnehmer* die oben genannten Anforderungen an die Storage-Anforderungen ebenfalls erfüllen.

9.6 Betriebssystem-Leistungen

Der *Auftragnehmer* installiert, konfiguriert, patcht und wartet die Betriebssysteme auf den durch ihn bereitgestellten physischen und virtuellen Server-Infrastrukturen. Dies umfasst die Implementierung von Sicherheitsupdates, die Überwachung der Systemleistung und die Behebung von Betriebssystemproblemen und Störungen. Das Betriebssystem muss den Vorgaben (siehe Anlage **02-02 Technologiegrundsätze**) des *Auftraggebers* entsprechen. Die betriebsrelevanten Parameter für die Infrastruktur-Landschaft sind in den service-spezifischen Betriebshandbüchern durch den *Auftragnehmer* zu dokumentieren und zu pflegen. Die oben genannten Leistungen sind unabhängig vom Bereitstellungsmodell zu erbringen.

9.7 Lizenz-Leistungen

Der *Auftragnehmer* stellt alle notwendigen Lizenzen und Wartungsvereinbarungen für die IT-Infrastruktur im Rahmen des Betreibermodells zur Verfügung. Das beinhaltet explizit, aber nicht ausschließlich, alle Betriebssysteme für die Server-Infrastruktur, Netzwerk-Connectivity Software, Backup- und Restore-Software, etc., außer es ist im Einzelnen explizit abweichend geregelt.

9.8 Virtuelle Systeme

Der *Auftragnehmer* übernimmt die Administration und sämtliche Betriebsthemen für die benötigten Hypervisor, um dem *Auftraggeber* virtuelle Maschinen bereitzustellen, welche die erforderlichen Betriebsparameter (beispielsweise Performance, Kapazität, Speicher und allen anderen relevanten Anforderungen) erfüllen. Der *Auftragnehmer* stellt die Virtualisierungssoftware bereit und sorgt für die Implementierung und Wartung. Regelmäßige Updates und Optimierungen der virtuellen Serverlandschaft werden durchgeführt, um die Leistungsfähigkeit und Sicherheit kontinuierlich zu verbessern. Alle Maßnahmen entsprechen den aktuellen technischen Standards und gesetzlichen Vorgaben.

Der *Auftragnehmer* stellt dabei insbesondere die Skalierbarkeit sicher, also die Fähigkeit, die Ressourcen (CPU, RAM, Speicher) dynamisch an die Anforderungen der virtuellen Maschinen anzupassen.

Der *Auftragnehmer* erstellt und verwaltet eine konsolidierte Kapazitäts- und Architekturdokumentation, die die Verknüpfungen zwischen virtuellen und physischen Servern sowie deren Umgebungen abbildet. Die zugehörigen Services ergeben sich aus Anhang **01-02-01 Servicekatalog**.

9.9 IT-Security

Der *Auftragnehmer* setzt im Rahmen seiner Leistungserbringung die IT-Security Anforderungen des *Auftraggebers* gemäß **01-02-01 Service Katalog**, grundlegende IT-Infrastrukturleistungen, SEC - Sicherheit, sowie **02-02 Technologiegrundsätze** um. Diese beinhalten:

- Gehärtetes System
- Schutz vor Schadsoftware
- Eindringungsschutz (IDS / IPS)
- Security Event
- Computer Emergency Response Team (CERT) Leistungen
- Schwachstellenscanning
- Firewall Management

9.10 Schwachstellen-Analyse

Der *Auftraggeber* behält sich das Recht vor, jährlich eine Schwachstellenanalyse durchzuführen, um mögliche Sicherheitslücken in der eingesetzten IT-Infrastruktur zu identifizieren, zu klassifizieren und zu bewerten. Der *Auftraggeber* leitet Maßnahmen aus der Schwachstellenanalyse ab. Der *Auftragnehmer* hat die Aufgabe, im Rahmen des kontinuierlichen Verbesserungsprozesses für die Managed Services die abgeleiteten Maßnahmen umzusetzen.

Weiterhin unterstützt die vom *Auftragnehmer* bereitgestellte Infrastruktur eine geeignete Antivirus-Software, die vom *Auftraggeber* betrieben werden kann.

9.11 Netzwerk-Leistungen und Anbindungs-Leistungen

Der *Auftragnehmer* ermöglicht die Verbindung der RZ-Leistungen mit dem Weitverkehrsnetz, welches vom *Auftraggeber* bereitgestellt wird. Die Installation von Netzwerkabschlussequipment in einem Carrierraum, sollte noch kein Übergabepunkt des Leitungsproviders im RZ vorhanden sein, wird ermöglicht. Sollten virtuelle Netzwerkappliances zum Einsatz kommen (Cloudbasierte RZ- Leistungen), wird der Betrieb in der entsprechenden Netzwerkzone ermöglicht. Die Compute- und Storageleistungen für das Hosting von virtuellen Netzwerk-Appliances (siehe **01-02 Servicekatalog** Virtuelle Systeme) sind in den Schätzmengen im **01-06 Leistungsverzeichnis** enthalten.

9.11.1 Firewall

Der *Auftragnehmer* stellt einen hochverfügbaren Firewallservice bereit. Die Firewall ermöglicht die Segmentierung der angebotenen Services auf Netzwerkebene, dient bei Netzübergängen innerhalb des Datacenters stets als Gateway und unterstützt sowohl Applikationserkennung als auch die Steuerung der Zugriffskontrolle anhand von Benutzer IDs. Sie überwacht und protokolliert den Netzwerkverkehr, um ungewöhnliche oder potenziell gefährliche Aktivitäten zu erkennen. Sie erlaubt die Trennung von Netzwerkbereichen, um den Zugriff zwischen verschiedenen Abteilungen oder Servern zu kontrollieren. Zudem bietet sie folgende Leistungen:

- Intrusion Detection und Prevention (IDS/IPS): Erkennung und Abwehr von Angriffen oder verdächtigen Aktivitäten innerhalb des Netzwerks.
- Schutz vor Schadsoftware: Überprüfung von Datenpaketen auf Viren, Würmer oder andere Malware.

Die Firewall soll zu Analysezwecken ein Logforwarding auf Logserver des *Auftraggebers* durchführen. Der *Auftragnehmer* implementiert die vom *Auftraggeber* gelieferten Sicherheitsrichtlinien.

9.11.2 Internet Access

Der *Auftragnehmer* stellt einen redundanten Zugang zum Internet bereit. Dieser ist kurzfristig auf Abruf verfügbar (Bereitstellung innerhalb von 5 Werktagen ab Abruf), stellt 10Gbps Bandbreite zur Verfügung, die in 10Gbps-Schritten auf maximal 100Gbps, innerhalb des o.g. Bereitstellungsfensters erhöht werden kann. Die Absicherung erfolgt durch ein vom *Auftraggeber* bereitgestellten Firewallcluster. Der Internetzugang muss über ein Tier 1-Peering in Deutschland bereitgestellt werden. Zudem stellt der *Auftragnehmer* ein öffentliches IP- Adressnetz bereit (Class C).

10 Leistungsbeschreibung der Arbeitsplatz Services

10.1 Client Release Management

Der *Auftraggeber* setzt aktuell 13 Client-Releases (Regel-In produktionsnahmen, kurz “Regel-IPN”) pro Jahr um. Ein entsprechendes Releasemanagement, nach den Vorgaben des *Auftraggebers*, ist zukünftig durch den *Auftragnehmer* umzusetzen. Von besonderer Bedeutung ist aufgrund von gesetzlichen Anpassungen und Änderungen das “Jahreswechsel-Release”, welches zwingend zum Stichtag zum 31.12. in der Produktion umgesetzt werden muss. Zusätzlich zu den definierten Releases muss die Möglichkeit bestehen, weitere Releases (Sonder-IPN) per Service Request zu beauftragen.

Die Umsetzung der jeweiligen Client-Releases erfolgt in vier aufeinanderfolgenden Phasen auf Fat-Clients sowie der Umgebung des virtuellen Arbeitsplatzes:

Phase	Beschreibung	Werktage	Anzahl Personen
QS	Hier werden eine Qualitätssicherung bzw. die Abnahme der bereitgestellten Pakete durchgeführt. Dafür stellt der *Auftragnehmer* entsprechende Teststellungen zur Verfügung. Während der QS-Phase müssen durch den *Auftraggeber* mitgeeilte Auffälligkeiten jederzeit vom *Auftragnehmer* behoben werden.	3-7	Ca. 1%
PreProd	Die PreProd-Phase findet innerhalb eines abgegrenzten Bereichs der produktiven Umgebung statt. Auffälligkeiten teilen die Tester dieser Phase per Incidentverfahren mit besonderer Reaktionszeit dem *Auftragnehmer* mit. Weiterhin ist an dieser Stelle ein Performancevergleich zu der aktuellen Produktion im Rahmen des virtuellen Arbeitsplatzes zu prüfen.	9	Ca. 5%
Prod	In dieser Phase erfolgt die Inproduktionsnahme (IPN) des Releases auf dem virtuellen Arbeitsplatz. Das Release für FatClients wird in durch		Alle

	den *Auftraggeber* definierten Rolloutwellen bereitgestellt.		
Hypercare	Sie dient dazu, nach der IPN auftretende Fehler schnell korrigieren zu können.	10	

Tabelle 5: Client Release Phasen

Ein "Sonder-Release" (Sonder-IPN) ist eine geplante, nicht-standardmäßige Freigabe von Software oder Software-Änderungen, die außerhalb des regulären Release-Zyklus oder der normalen Planung erfolgt. Es kann sich um neue Funktionen, Erweiterungen oder Änderungen an bestehenden Software-Lösungen handeln.

Außerhalb der durch den *Auftraggeber* geplanten Releases muss es zu jeder Zeit möglich sein, anlassbezogene Updates (z.B. zum Schließen von kritischen Sicherheitslücken) in kürzeren Intervallen zu verteilen, Details siehe Anforderungen in Kapitel 10.4.2. Software Paketierung.

10.2 Virtueller Arbeitsplatz

Der Service Virtueller Arbeitsplatz bietet Nutzern flexible und skalierbare Desktop-Lösungen für personalisierte und geteilte („pooled“) Instanzen, die einen sicheren Zugriff auf eine vollständige Arbeitsumgebung ermöglichen – unabhängig von Gerätetyp und Standort. Der Service unterstützt die Flexibilität und Mobilität der Mitarbeiter des *Auftraggebers* und ist ideal für hybride und remote Arbeitsmodelle.

Die aktuelle Terminalserver Architektur soll abgelöst und durch eine Virtual Desktop Infrastructure (VDI) ersetzt werden. Im Rahmen dieser Ausschreibung umfasst der Service die Beschaffung und Bereitstellung von virtuellen Arbeitsplätzen, welche in einer Virtual Desktop Infrastructure betrieben werden. Diese virtuelle Arbeitsumgebung basiert auf dem aktuellen Windows Client Betriebssystem.

Der *Auftraggeber* ist grundsätzlich technologieoffen. Der *Auftragnehmer* hat die Möglichkeit, verschiedene VDI-Technologien zu evaluieren und dem *Auftraggeber* als Lösung anzubieten.

Der *Auftragnehmer* stellt virtuelle Arbeitsplätze bereit und ermöglicht den Mitarbeitern des *Auftraggebers* den Zugriff auf die virtuellen Arbeitsplätze von den Standorten des *Auftraggebers* und über das Internet (z.B. aus dem Home-Office). Hierbei erfolgt der Zugriff mit Managed Windows/Apple/Igel- Clients als auch mit Windows/Apple BYODs.

10.2.1 Allgemeine Technologieinformationen

Der Service Virtueller Arbeitsplatz beinhaltet die Varianten “Non-Persistent Pooled Virtual Desktop” und “Persistent Virtual Desktop”, die nachfolgend beschrieben sind.

Der *Auftraggeber* hat ca. potentielle 18.000 Nutzer für den Service Virtueller Arbeitsplatz. Der “Non-Persistent Pooled Virtual Desktop” wird von derzeit maximal 11.000 Nutzern gleichzeitig genutzt. Der “Persistent Virtual Desktop” wird von derzeit maximal 1.100 Nutzern gleichzeitig genutzt.

Folgende Funktionen müssen unterstützt werden:

- Die Virtual Desktops müssen auf dem aktuellen und durch Microsoft supporteten Windows Client Enterprise Betriebssystem (aktuell Windows 11 Enterprise) basieren.
- Die Virtual Desktops werden mit Softwarepaketen aus dem Service Software-Management versorgt.
- Die Bereitstellung soll in logisch getrennten Zonen (Entw/QS - PreProd/Prod) erfolgen.

10.2.2 Non-Persistent Pooled Virtual Desktop

Der Ansatz soll folgende Funktionen unterstützen:

- Die Virtual Desktops dürfen nicht durch den User veränderbar sein.
- Die Virtual Desktops werden durch Reboot auf den Initialzustand zurückgesetzt.
- Die Bereitstellung soll in logisch und physisch getrennten Zonen (Entw/QS - Pre-Prod/Prod) erfolgen.

10.2.3 Persistent Virtual Desktop

Der Ansatz soll folgende Funktionen unterstützen:

- Zusätzliche Software-Produkte müssen über den Service Software-Management installierbar sein.
- Die Festplatten der Virtual Desktops müssen persistent sein.
- Ein Virtual Desktop soll auch mehreren Benutzern zur Verfügung gestellt werden können.
- Persistent Virtuelle Desktops können durch Benutzer dauerhaft verändert werden.
- Einzelne Virtual Desktops müssen zu einem Cluster zusammenfassbar sein, um hieraus eine “Pooled Bereitstellungsgruppe” zu bilden (Persistent Pooled Virtual Desktop).

10.2.4 Allgemeiner Funktionsumfang

Der virtuelle Arbeitsplatz stellt eine Umgebung auf Basis des aktuellen durch Microsoft im Support befindlichen Client-Betriebssystems (aktuell Windows 11 Enterprise 24H2) bereit.

Dabei werden alle Standardfunktionen von Windows unterstützt - insbesondere:

- **Netzwerkdruck**: Nahtlose Integration für netzwerkgebundene Drucker (siehe Kapitel 10.5 Arbeitsplatzdruck).
- **Dateiverwaltung**: Zugriff auf Speicherressourcen (siehe Kapitel 11.1 File Services) sowie die Möglichkeit zur Dateiübertragung innerhalb der Umgebung des Auftraggebers.
- **Benutzerprofile**: Persistente Benutzerprofile, die eine konsistente Arbeitsumgebung ermöglichen (siehe Kapitel 2.2.3 im Anhang **01-03 Technologiedefinitionen**).

10.2.5 Anwendungen

Der *Auftragnehmer* stellt in den virtuellen Arbeitsplätzen die Applikationen des *Auftraggebers* bereit. Die Anwendungszuordnung erfolgt rollenbasiert aus dem IAM des *Auftraggebers*. Wichtige Unternehmensanwendungen sind:

- **Genesys (WDE Client)**: Contact-Center Lösung (Call-Center) für den Kontakt mit den Kunden (Versicherte) des *Auftraggebers*.
- **SAP GUI**: Nutzung der SAP-Client-Anwendungen.
- **bCare**: Eigenentwicklung des *Auftraggebers* für Anwendungen mit u.a. den Modulen / Sub-Anwendungen: Elvis, VM-EVA, DiMaP, AMRAC, Karma, ZLF.
- **Sprach- und Kollaborationsdienste WebEx/MS Teams**: Bereitstellung und Betrieb von Anwendungen für die Kommunikation und Kollaboration inkl. erforderlicher lokaler Beschleunigung auf dem Anwendergerät (z.B. VDI-Plugins).
- **Webbrowser** inkl. Nutzbarkeit für Videostreaming-Plattformen, Meeting-Plattformen und rechenintensiven Anwendungen wie SAP-Fiori.
- **Weitere geschäftsrelevante Software**: Installation weiterer Anwendungen, die für die spezifischen Aufgaben der Nutzer erforderlich sind.

Die Liste aller Anwendungen des *Auftraggebers* ist in Anlage **01-09 Assets** zu finden.

10.2.6 Zugriff auf virtuelle Arbeitsplätze

Nachfolgend sind grundlegende Anforderungen an den Zugriff auf die durch den *Auftragnehmer* bereitgestellten virtuellen Arbeitsplätze beschrieben:

- Der Zugriff auf die virtuellen Arbeitsplätze erfolgt aus Standorten des *Auftraggebers* und über das Internet (z.B. aus dem Home-Office, mobiles Arbeiten).
- Dieser Zugriff erfolgt mit Thin-, Fat-Clients und “Managed Mobile Devices” in einer Kombination mit einer Remote-Access-Applikation (aktuell Citrix Workspace), die vom *Auftraggeber* bereitgestellt wird.
- Die Lösung ermöglicht eine Nutzung von Clients mit geringen Hardwareanforderungen.
- Der *Auftragnehmer* muss sicherstellen, dass die Thin-Clients des *Auftraggebers* in der neuen Lösung vollumfänglich arbeitsfähig sind. Die aktuell eingesetzten Thin-Clients sind mit einem Celeron Prozessor, 8 GB Arbeitsspeicher und 128 GB SSD ausgerüstet.
- Der Zugriff für Bring-Your-Own-Devices (BYOD) als Fallback für die Remote-Access-Applikation muss per HTML5 möglich sein. Der Support für Bring-Your-Own-Devices ist nicht Gegenstand der Leistungserbringung.
- Es muss möglich sein, Computer-Last auf die Endgeräte auszulagern. Dies gilt insbesondere, wenn die Abarbeitung dieser Last in der Infrastruktur zu negativen Auswirkungen in der User Experience auf Grund von Verzögerungen in der Übertragung führt, wie dies regelmäßig bei Audiodatenströmen oder multimedialen Inhalten der Fall ist. Hierunter fallen VDI-Plugins für WebEx, Teams und Technologien zur Content-redirection.

10.2.7 Allgemeine Anforderungen an die Leistungserbringung

Nachfolgend werden allgemeine Anforderungen an die Leistungserbringung durch den *Auftragnehmer* zum Virtual Desktop beschrieben:

- Die Virtual-Desktop-Infrastruktur muss App-Streaming-Lösungen und App-Publishing-Lösungen unterstützen.
- Der *Auftragnehmer* stellt sicher, dass die angebotene Lösung alle Anwendungen des *Auftraggebers* (siehe Anlage **01-09 Assets**) unterstützt und auf dieser Lösung durch den Hersteller der Anwendungen supportet wird. Wenn dieser Support durch den Hersteller nicht gegeben ist, muss der Auftragnehmer den Support erbringen.
- In diesem Sinne umfasst „Support“ sämtliche Maßnahmen, die der *Auftragnehmer* zur Sicherstellung des ordnungsgemäßen Betriebs, der Wartung und der Fehlerbehebung der Anwendung erbringt, sofern für die auf der angebotenen Lösung betriebene Anwendung kein Hersteller-Support besteht. Dieser Support beinhaltet:
    - **Betriebsfähigkeit und Kompatibilität**: Der *Auftragnehmer* gewährleistet die Funktionsfähigkeit der Anwendung auf der angebotenen Lösung und übernimmt die Verantwortung für deren Kompatibilität.
    - **Fehleranalyse und -behebung**: Der *Auftragnehmer* stellt sicher, dass auftretende Fehler innerhalb definierter Reaktions- und Lösungszeiten analysiert und behoben werden.
    - **Bereitstellung von Updates & Patches**: Sofern erforderlich, entwickelt oder implementiert der *Auftragnehmer* geeignete Maßnahmen zur Fehlerbehebung, einschließlich Patches, Updates oder Workarounds.
    - **Supportstruktur und Erreichbarkeit**: Der *Auftragnehmer* stellt eine Supportstruk-

tur zur Verfügung (inkl. Ticketsystem, Hotline) und definiert klare Kommunikationswege sowie Reaktionszeiten für die Bearbeitung von Anfragen.
    - **Sicherstellung der Betriebskontinuität**: Der *Auftragnehmer* ergreift proaktive Maßnahmen zur Vermeidung von Störungen und stellt gegebenenfalls alternative Betriebs- oder Migrationsstrategien bereit.
- Der *Auftragnehmer* stellt sicher, dass der Service mit den in Anhang **01-04 Service Levels** definierten Verfügbarkeits-Klassen und Wiederherstellungszeiten betrieben wird.
- Der *Auftragnehmer* stellt sicher, dass die Performance den im Anhang **01-04 Service Levels** definierten Anforderungen entspricht.

10.2.8 Skalierbarkeit und Flexibilität

Der Service muss ein hohes Maß an Skalierbarkeit und Flexibilität bieten, um sowohl kurzfristige Änderungen als auch langfristige Wachstumsstrategien zu unterstützen. Die Lösung für die virtuellen Arbeitsplätze ist vom *Auftragnehmer* darauf auszulegen, dass eine flexible Anpassung an die tatsächliche Anzahl von gleichzeitigen Benutzern möglich ist. Dies umfasst:

- Der Service wird durch den *Auftragnehmer* für eine parallele Nutzung von bis zu 11.000 gleichzeitigen Nutzern bereitgestellt.
- Des Weiteren muss die Lösung vom Auftragnehmer so konzipiert werden, dass bei Bedarf eine um 30% erhöhte Anzahl von Benutzern bei gleicher Performance sichergestellt ist (Skalierbarkeit).

10.2.9 Betrieb und Management

Der *Auftragnehmer* ist zum Betrieb und Management der Virtual Desktop Infrastructure (VDI) verpflichtet. Der *Auftragnehmer* muss die Infrastruktur professionell und zuverlässig verwalten. Die zentralen Aspekte der Betriebs- und Managementleistungen des *Auftragnehmers* sind wie folgt:

10.2.9.1 Betrieb und Monitoring der Lösung

Der *Auftragnehmer* übernimmt die vollständige Administration, den Betrieb und Releasetätigkeiten (siehe Kapitel 10.1 Client Release Management) für die virtuellen Arbeitsplätze. Dies umfasst:

- **Monitoring und Überwachung**: Ständige Überwachung der Systemperformance und -verfügbarkeit zur frühzeitigen Identifikation und Behebung von Problemen, wie detailliert in Anlage **02-02 Technologiegrundsätze** beschrieben.
- **Patch- und Update-Management**: Regelmäßige Updates und Sicherheits-Patches (sowohl für das Backend-System als auch für die Windows-Betriebssystem-Ebene für die Nutzer), die außerhalb der definierten Betriebszeiten implementiert werden, um Unterbrechungen der Arbeitsabläufe zu vermeiden. Diese sind in der Regel mit den definierten Releasezyklen zu harmonisieren. Siehe Anlage **02-02 Technologiegrundsätze**.
- **Verwaltung der Gruppenrichtlinien**: Übernahme und Pflege von GPOs (Group Policy Objects) (siehe Kapitel 10.4 ff. Software-Management).
- **Kapazitätsmanagement**: Sicherstellung, dass ausreichend Ressourcen für die Bereitstellung der benötigten Leistung zur Verfügung stehen.
- **Hypervisor Virtualisierung:** Der *Auftragnehmer* stellt eine oder mehrere Schnittstellen bereit, über die berechtigte Benutzer Daten bzgl. des Monitorings abrufen können. Vom *Auftraggeber* benannte Mitarbeiter haben Zugang zum Live-Monitoring u.a. zu Storage, Clustering, Disaster Recovery, Backups, Portbelegung.

10.2.9.2 Wartung und Störungsbehebung

- **Wartungsarbeiten**: Geplante Wartungsarbeiten erfolgen außerhalb der im Anhang **01-04 Service Level** definierten Servicezeiten, um den laufenden Betrieb der Arbeitsplätze nicht zu beeinträchtigen.
- **Störungsmanagement**: Der *Auftragnehmer* ist verpflichtet, Störungen innerhalb der vereinbarten Service Level zu beheben. Eine detaillierte Definition von Reaktions- und Lösungszeiten wird über das Service Level Agreement (SLA) und Service Level Targets geregelt. Nach Durchführung eines Releases (siehe Kapitel 11.1 Client-Releasemanagement) muss eine HyperCare-Phase durch den *Auftragnehmer* sichergestellt werden.

10.3 Office Arbeitsplatz

Der Office Arbeitsplatz ist eine Arbeitsumgebung für klassische Windows Fat-Clients (siehe Assets in Anlage **01-09 Assets**). Mit Fokus auf Performance, Sicherheit und Standardisierung stellt der Service sicher, dass Mitarbeiter des *Auftraggebers* effektiv arbeiten können. Der *Auftragnehmer* übernimmt für den Service Office Arbeitsplatz die Bereitstellung, die Verwaltung und die kontinuierliche und regelmäßige Aktualisierung und Optimierung der Arbeitsplatzumgebung, Betriebssysteme und Anwendungen (Evergreen-Strategie).

Nachfolgend werden wesentliche Komponenten der Leistungserbringung durch den *Auftragnehmer* zum Office Arbeitsplatz beschrieben:

- **Installation und Konfiguration:** Der Windows FAT-Client wird über den Microsoft Configuration Manager installiert und konfiguriert. Dabei kommt ein Softwarelayer-Modell zum Einsatz, das eine strukturierte Bereitstellung und Wartung der Systeme ermöglicht.

Bereitstellung des Betriebssystems: Das Betriebssystem wird auf Basis eines standardisierten Software-Images ausgerollt. Die Endgeräte müssen mit einem aktuellen Windows Betriebssystem betrieben werden, welches sich bei Microsoft in der Mainstream Supportphase befindet. Derzeit wird Windows 11 Enterprise 24H2 eingesetzt. Regelmäßige Patches und Updates sorgen für eine aktuelle und sichere Umgebung. Der *Auftraggeber* ist in regelmäßigen Abständen vor einer Aktualisierung des Betriebssystems zu informieren, der *Auftraggeber* stellt hierfür Testgeräte zur Verfügung.

- **Installation betriebssystemnaher Systemkomponenten:** Neben dem eigentlichen Betriebssystem werden essenzielle Systemkomponenten installiert, darunter z.B.
  - NET Framework
  - Microsoft Visual C++ Redistributable Packages
  - Weitere erforderliche Laufzeitbibliotheken und Systemerweiterungen
- **Integration der Standardsoftware:** Zusätzlich wird eine Auswahl an Standardsoftware installiert, um eine einheitliche Arbeitsumgebung sicherzustellen:
  - Adobe Reader (für PDF-Dokumente)
  - 7-Zip (für Archivierung und Komprimierung)
  - Microsoft Office 365 (für produktive Büroanwendungen)
  - Weitere relevante Softwarepakete je nach Unternehmensanforderung
- **Benutzerdefinierte Anpassungen:** Außerdem werden benutzerdefinierte Anpassungen auf den Endgeräten vorgenommen, darunter u.a.
  - Wallpaper
  - Energiesparoptionen

- Diverse Gruppenrichtlinien

Die gesamte Installation bildet die Basisinstallation für alle Clients und stellt eine einheitliche Grundlage für alle Systeme sicher. Nach jedem Software-Release wird diese Basisinstallation auf den jeweils aktuellen Stand gebracht, sodass alle enthaltenen Komponenten, Systembibliotheken und Anwendungen stets den neuesten Versionsstand aufweisen. Dadurch wird gewährleistet, dass bei einer Neuinstallation eines Clients immer die aktuelle und vollständig gepatchte Softwareumgebung bereitgestellt wird. Diese strukturierte Vorgehensweise sorgt für eine effiziente und standardisierte Bereitstellung von Windows-FAT-Clients im Unternehmen.

FAT-Clients werden auch für Personen mit körperlichen Einschränkungen eingesetzt. Dafür sind hier spezielle Peripheriegeräte (z.B. Braile Tastatur, XXL Monitor, spezielle Mäuse, Diktiergeräte etc.) zu unterstützen. Diese Peripheriegeräte werden durch den *Auftraggeber* beigestellt. Die notwendigen Treiber für vorhandene Peripheriegeräte stellt der *Auftraggeber* zur Verfügung. Für neue Peripheriegeräte beschafft der *Auftragnehmer* die Treiber und integriert diese in das Betriebssystem-Image.

Der *Auftragnehmer* stellt grundsätzlich vollautomatisierte Softwareinstallationen bereit, die auf den Endgeräten verteilt werden. Innerhalb der Arbeitsumgebungen gibt es jedoch spezifische Anwendungsfälle, die manuelle Eingriffe oder Nacharbeiten an den entsprechenden Endgeräten erfordern. Dazu zählen Installationen, die nicht automatisiert durchgeführt werden können, VIP-Support oder die Konfiguration von Spezialanwendungen. Für diese Tätigkeiten sind lokale administrative Berechtigungen an den Endgeräten erforderlich, die den Vor-Ort-Service-Mitarbeitern oder berechtigten Administratoren des *Auftraggebers* zur Verfügung gestellt werden müssen.

Der *Auftragnehmer* wird folgende Leistungen erbringen:

- Die Kompatibilität der zu betreibenden Systeme mit neuen Hardwaregenerationen der beim *Auftraggeber* eingesetzten Hardware kontinuierlich überprüfen.
- Automatisierte Durchführung von Betriebssystem- und Softwareupdates, um die Arbeitsplätze auf dem neuesten Stand zu halten und die Sicherheit zu gewährleisten. Diese werden in festgelegten Releasezyklen umgesetzt (siehe Kapitel 11.1 Client-Releasemanagement).
- Erstellung und Pflege von Gruppenrichtlinien. Kontinuierlich werden auf Anforderungen des *Auftraggebers* in Abstimmung mit dem *Auftragnehmer* Sicherheitsanforderungen und Konfigurationen umgesetzt.
- Erstellung und Pflege von Logonscripts
- Installation und Verteilung von Updates der benötigten Basis-Anwendungen, darunter insbesondere Microsoft Office und weitere Arbeitswerkzeuge. (siehe Anlage **01-09 Assets**).
- Die aktualisierte Basisinstallation wird dann in die jeweilige neue Task-Sequenz im Microsoft Configuration Manager integriert. Dynamisch zugewiesene Treiberpakete vervollständigen die OS-Task-Sequenz. Diese Vorgehensweise bietet den Vorteil, dass die Installation von FAT-Clients schnell und effizient durchgeführt werden kann.
- Der *Auftragnehmer* nutzt für das Software-Management den Microsoft Configuration Manager (MCM), für den der *Auftraggeber* die Lizenzen beistellt (siehe Kapitel 10.4 ff. Software-Management).
- Durchführung regelmäßiger Wartungsmaßnahmen in Bezug auf Software Aktualisierung und Patchverteilung, um eine optimale Funktion der Arbeitsplätze zu gewährleisten. Der *Auftraggeber* erhält auf Anforderung einen Report zu den durchgeführten Wartungsmaßnahmen.

- Sollte der *Auftragnehmer* im Rahmen der Wartungsmaßnahmen als kritisch einzustufende Erkenntnisse gewinnen, so informiert er den *Auftraggeber* unverzüglich. Sollten sicherheitsrelevante (IT-Security) Erkenntnisse auftreten, informiert der *Auftragnehmer* den *Auftraggeber* ebenfalls unverzüglich.

10.4 Software-Management

Der Service Software-Management bietet Funktionen zur Paketierung, automatisierten Verteilung, Verwaltung und Wartung von Betriebssystemen und Software auf den Endgeräten (Service Office Arbeitsplatz und Service virtueller Arbeitsplatz) des *Auftraggebers*.

10.4.1 Endpoint Management

Der *Auftragnehmer* stellt für die automatisierte Verteilung von Betriebssystemen, Treibern, Softwarepaketen/-updates und Patches und für die Verwaltung der Endgeräte des *Auftraggebers* (Service Office Arbeitsplatz und Service virtueller Arbeitsplatz) ein Deployment-System bereit und ist für dessen Betrieb verantwortlich. Aus dem existierenden Deployment-System (Microsoft Configuration Manager) des *Auftraggebers* sind durch den *Auftragnehmer* alle Konfigurationen und Funktionen zu übernehmen. Das Management aller virtuellen und physischen Endgeräte, gelistet in Anlage **01-09 Assets**, umfasst:

- Installation und Verteilung von Betriebssystemen.
- Zurücksetzen und Neuaufsetzen von Clients.
- Sicherstellung der Treiberkompatibilität und Durchführung von Hardware-Zertifizierungen.
- Inventarisierung von Hardware und Software

Field-Services zum Management der Endgeräte liegen in der Verantwortung des *Auftraggebers* und sind nicht Bestandteil dieser Ausschreibung.

10.4.1.1 Endpoint Management Infrastruktur

Das Deployment-System besteht aus zentraler und dezentraler Infrastruktur. Die zentrale Infrastruktur besteht aus:

- Primärer Standortserver (Primary Site Server)
- SQL Server
- Management Point (MPs)
- Distribution Point (DPs)
- Software Update Point (SUP)

Die dezentrale Infrastruktur besteht aktuell aus 13 Distribution Points, welche an Standorten mit mehr als 30 Endgeräten eingerichtet sind. Die vorhandene Netzwerkbandbreite wird als ausreichend eingestuft. Der *Auftragnehmer* soll sicherstellen, dass die Softwarepakete an diesen Standorten zwischengespeichert und effizient verteilt werden. Eine Übersicht der Distribution Points liegt im Anlage **01-09 Assets** vor.

Der *Auftragnehmer* muss das Deployment-System an das Cloud Management Gateway (CMG) des *Auftraggebers* anbinden. Das Cloud Management Gateway (Betrieb durch den *Auftraggeber*) unterstützt die Softwareverteilung im Home-Office und an Standorten mit geringer Netzwerkbandbreite.

10.4.1.2 Rollen und Berechtigungen

Der *Auftragnehmer* muss ein Rollenmodell im Softwaredeployment implementieren, welches Be-

standteil der zu übernehmenden Funktionen aus dem bestehenden Deployment-System ist. Dieses ermöglicht es dem *Auftraggeber* sowie den Dienstleistern des User-Helpdesks, Warenkorbs und Field-Services, Standardaufgaben wie die Reparatur von Softwarepaketen, die Neuinstallation von Clients, die Steuerung von Task Sequences und den lesenden Zugriff für Reporting-Zwecke durchzuführen.

Die Rollen sind so zu gestalten, dass eine sichere und effiziente Nutzung gewährleistet ist. Zudem sollen die Berechtigungen granular definiert werden, um eine klare Trennung zwischen administrativen und anwendungsbezogenen Rechten sicherzustellen. Die spezifischen Rollen werden durch den *Auftraggeber* vorgegeben.

10.4.1.3 Skalierbarkeit

Sofern die angebotene Endpoint Management Infrastruktur nicht cloudbasiert ist, soll diese die perspektivisch mögliche Migration zu cloudbasierten Endpoint Management Lösungen (z.B. Intune) unterstützen.

10.4.2 Software Paketierung

Der *Auftragnehmer* übernimmt die Paketierung, die Entwicklertests und automatisierte Verteilung von Software (Standard Software, angepasste Standard Software, Eigenentwicklungen des *Auftraggebers*, Updates und Security Patches) auf die Endgeräte (Service Office Arbeitsplatz und Service virtueller Arbeitsplatz) des *Auftraggebers*. Die Fristen für die Verteilung der Softwarepakete sind im Anhang **01-04 Service Levels** definiert.

Die aktuell genutzten Softwarepakete basieren auf den Tools PSAppDeployToolkit und Microsoft PowerShell. Der *Auftraggeber* stellt die aktuell genutzten Softwarepakete initial bei (**01-09 Assets**). Der *Auftragnehmer* muss diese Lösung als Standard für die Software-Paketierung weiterverwenden.

Der *Auftragnehmer* stellt eine Austauschplattform bereit. Über diese werden Softwarequelldateien und Installationsanleitungen durch den *Auftraggeber bereitgestellt*. Der *Auftragnehmer* speichert Softwarepakete in allen Versionen und zugehörigen Softwarepaketdokumentationen auf der Austauschplattform.

Der *Auftragnehmer* verwaltet und dokumentiert die Softwarepakete revisionssicher in der obengenannten Austauschplattform. Der *Auftraggeber* hat Zugriff auf die Dokumentationen, Quellcodes und alle weiteren Informationen zu den erstellten Softwarepaketen. Diese können via Web-Zugriff und API abgerufen werden.

Nach Ende der Vertragslaufzeit gehen alle während dieser Zeit erstellten Softwarepakete in den Besitz des *Auftraggebers* über und sind vom *Auftragnehmer* zu übergeben.

Die Paketierung erfolgt in drei Kategorien mit einfachen, mittleren und komplexen Softwarepaketen.

10.4.2.1 Software Paketierung Kategorie Einfach

Zum Software Paket Kategorie Einfach gehören Standardanwendungen oder einfache Tools mit folgenden Merkmalen:

- Einfache EXE oder MSI Dateien mit Standard-Installationsparametern
- Kein dynamischer Dateizugriff
- Keine DLL-Auflösung
- Kein Dateisperrkonflikt

- Standard Security
- Keine Benutzerdefinierte Registry-Updates
- Keine Reboots
- Keine Verschlüsselung
- Kein Passwort

10.4.2.2 Software Paketierung Kategorie Mittel

Zum Software Paket Kategorie Mittel gehört Software mit zusätzlicher Konfiguration mit folgenden Merkmalen:

- Installation benötigt zusätzliche Parameter
- Voreinstellungen müssen verteilt werden
- Kein dynamischer Dateizugriff
- Wenige DLL-Auflösungen
- Wenige nicht-selbstregistrierende Dateien
- Mögliche Dateisperrkonflikt
- Standard Security
- Abhängige Installationen sind vorhanden
- Wenige Benutzerdefinierte Registry-Updates
- Einzelne Reboots
- Mit Verschlüsselung
- Mit Passwort

10.4.2.3 Software Paketierung Kategorie Komplex

Zum Software Paket Kategorie Komplex gehört Software mit umfangreichen Konfigurationen mit folgenden Merkmalen:

- Viele Installationsoptionen sind modifiziert
- Dynamischer Dateizugriff
- Ausführen von Post-Installationen ist erforderlich
- Viele DLL-Auflösungen
- Viele nicht-selbstregistrierende Dateien
- Mögliche Dateisperrkonflikt
- Nicht-Standard Security
- Viele Abhängigkeiten sind vorhanden
- Viele Benutzerdefinierte Registry-Update
- Mehrfache Reboots
- Mit Verschlüsselung
- Mit Passwort

Jede der obengenannten Softwarepaket Kategorien kann zusätzlich als Emergency Patch beauftragt werden. Hierbei handelt es sich um eine Software-Management Leistung für zu paketierende Software mit beschleunigter Bereitstellung. Dabei handelt es sich um sicherheitsrelevante Updates oder Patches zur Behandlung von Schwachstellen mit hoher Kritikalität oder um anwendungsspezifische Änderungen mit hoher Dringlichkeit.

Der Freigabeprozess für die Software Paketierung ist im Kapitel 10.1 Client-Releasemanagement beschrieben.

10.4.3 Software Verteilung

Mit dem Deployment-System werden bereits ausgerollte Softwarepakete aktualisiert sowie neue Softwarepakete und Sicherheits-Patches durch den *Auftragnehmer* auf die Endgeräte des *Auftraggebers* (Service Office Arbeitsplatz und Service virtueller Arbeitsplatz) verteilt.

Die aktuell genutzten Softwarepakete sind in Anlage **01-09 Assets** hinterlegt. Die Verteilung der Softwarepakete erfolgt automatisiert über ein Deployment-System (siehe Kapitel 10.4.1 Endpoint Management).

Nachfolgend sind die wesentlichen Aufgaben des *Auftragnehmers* im Rahmen der Softwareverteilung beschrieben:

- Verteilung von Softwarepaketen an unterschiedliche Nutzergruppen und Gerätetypen (Service Office Arbeitsplatz und Service virtueller Arbeitsplatz). Die Zuordnung von Softwarepaketen zu Nutzern und deren Verteilung erfolgt dabei auf Basis von Active Directory- bzw. Entra-ID Gruppen bzw. einzelnen Nutzern des *Auftraggebers*.
- Verteilung und Pflege von Gruppenrichtlinien für die virtuelle Arbeitsplatzumgebung sowie der Windows FAT-Client Installationen unter Berücksichtigung der vom *Auftraggeber* beauftragten Konfigurationen. Weiterhin werden vom *Auftragnehmer* regelmäßige Sicherheitsanforderungen zwecks Aktualisierung der Baseline und Hardening-Policies vorgenommen, welche in Abstimmung und inklusive Tests mit dem *Auftraggeber* stattfinden.
- Die monatlichen und regelmäßigen Releases (IPNs, siehe Kapitel 10.1) müssen in Wellen durchgeführt werden. Diese Wellen sind mit dem *Auftraggeber* abzustimmen.
- Der *Auftragnehmer* ist für die Entstörung von fehlerhaft installierten Softwarepaketen verantwortlich, sofern diese fehlerhaft installiert wurden und der Fehler nicht auf die Applikation zurückzuführen ist.
- Der *Auftragnehmer* bringt die Pakete des *Auftraggebers* so aus, dass der Anwender Einfluss auf den Installationszeitpunkt hat (z.B. Hinweis am Client auf anstehende Installation mit der Möglichkeit, die Installation für einen begrenzten Zeitraum dreimal zu verschieben).
- Ist im Rahmen der Installation ein Neustart des Rechners erforderlich, so muss ein zu diesem Zeitpunkt angemeldeter Anwender die Möglichkeit haben, den Zeitpunkt zu beeinflussen (z.B. Hinweis am Client auf erforderlichen Neustart mit der Möglichkeit, den Neustart bis zu dreimal für einen begrenzten Zeitraum auf einen passenderen Zeitpunkt zu verschieben).
- Der *Auftragnehmer* muss ein Verfahren bereitstellen, einen automatischen Neustart im Rahmen von Installationen bei vom *Auftraggeber* benannten Rechnern (z.B. Entwickler Arbeitsplätze) auch dann zu unterbinden, wenn kein Anwender an diesem Rechner angemeldet ist. Diese Rechner werden im Rahmen der Feinkonzeption festgelegt.
- Kann der *Auftragnehmer* die Softwareverteilung nicht automatisiert gestalten, ist der *Auftragnehmer* zu manuellen Installationen oder ggf. manuellen Nacharbeiten verpflichtet.
- Der *Auftragnehmer* ist verpflichtet, Updates oder Patches gemäß den Vorgaben in dem Kapitel 9.4 Patch Management mit dem *Auftraggeber* einzuspielen.

Die folgenden Anforderungen an die Softwareverteilung sind durch den *Auftragnehmer* umzusetzen:

- Es sind regelmäßige Abstimmungen mit dem *Auftraggeber* durchzuführen.
- Es soll möglichst keine Benutzerinteraktion erforderlich sein.
- Es sollen möglichst keine Pop-Ups auf dem Bildschirm angezeigt werden.

- Es soll eine möglichst geringe Anzahl an Reboots verwendet werden.
- Sicherheitspatches sind auch außerhalb der monatlichen Releases und in Absprache mit dem Auftragnehmer zu verteilen. Dies umfasst sowohl Patches von Microsoft Sicherheitslücken als auch Patches von 3rd Party Sicherheitslücken.
- Basisanwendungen (z.B. Microsoft Windows, Microsoft M365 Apps for Enterprise, 7-Zip, Adobe Reader, Notepad++, Google Chrome, PDF24, OpenJDK, Citrix Workspace, WIN SCP, VLC Media Player und KeePass XC) sind durch den *Auftragnehmer* kontinuierlich zu aktualisieren.

10.5 Arbeitsplatz Druck

Der Service Arbeitsplatzdruck des *Auftraggebers* umfasst die Bereitstellung, die Implementierung, den Betrieb und die Administration von Multifunktionsprinter (MFPs) und Druckservern und der zur Erbringung des Service sonstigen erforderlichen IT-Komponenten. Es wird ausdrücklich darauf hingewiesen, dass der erforderliche Funktionalitätsumfang in Anhang **01-03 Technologiedefinitionen** beschrieben ist. Ein vollständiges Bild zu den Anforderungen und Rahmenbedingungen des Service Arbeitsplatz Druck ist nur im Zusammenspiel der Ausführungen in dieser Leistungsbeschreibung und in den Technologiedefinitionen sichtbar.

Der *Auftraggeber* verfolgt dabei das Ziel, für den Druck an den Arbeitsplätzen und aus den Fachanwendungen einen Printservice zur Verfügung zu stellen, der

- die Einhaltung gesetzlicher und hauseigener Compliancevorgaben (siehe Anlage **02-09-03 AVV TOMs Informationssicherheit**) gewährleistet,
- verlässlich, stabil und performant ist,
- kosteneffizient und bzgl. der Kosten nachvollziehbar ist,
- innovative und zukunftsgerichtete Technologien verwendet,
- flexibel bereitgestellt wird und an die sich ändernden geschäftlichen Erfordernisse angepasst werden kann.

Hierzu erwartet der *Auftraggeber* das proaktive Aufzeigen von Optimierungsmöglichkeiten des *Auftragnehmers* während der Vertragslaufzeit.

10.5.1 Services für den Arbeitsplatzdruck

Der *Auftragnehmer* stellt dem *Auftraggeber* die nachfolgend beschriebenen IT-Services zur Verfügung. Die Services des *Auftragnehmers* umfassen das zentral erbrachte Engineering, Management und den zentralen Betrieb einer Lösung für den Arbeitsplatzdruck, welche den Anforderungen in **01-03 Technologiedefinitionen** genügt. Der *Auftragnehmer* ist für die Erbringung des 2nd Level Support und des 3rd Level Support für die Services verantwortlich.

Im Rahmen dieses Service stellt der *Auftragnehmer* für die durch den *Auftraggeber* bereitgestellten Drucker und Multifunktionsgeräte eine zentrale Druckinfrastruktur für den Arbeitsplatzdruck zur Verfügung. Der *Auftragnehmer* verantwortet die Konfiguration der eingesetzten Druckertreiber. Die Installation der Druckertreiber erfolgt durch den *Auftragnehmer*.

Die Entwicklung und Vorgabe der Konfigurationsparameter der Druckgeräte inklusive Peripherie (unter anderem Firmware, Geräteeinstellungen und Embedded Software wie z.B. Client einer „Vertrautes Drucken“ Lösung, inklusive Verschlüsselung) ist ebenso Aufgabe des *Auftragnehmers*. Diese Vorgaben sind mit dem *Auftraggeber* so weit abzustimmen, dass sie mit dessen geschäftlichen Erfordernissen übereinstimmen.

Die Bestandsverwaltung (Drucker, MFPs) obliegt dem *Auftraggeber*. Für die remote-Administration dieser Geräte erforderliche Bestandsdaten werden zwischen *Auftraggeber* und *Auftragnehmer* abgestimmt und aus dem bestandsführenden System des *Auftraggebers* übermittelt.

Der *Auftraggeber* (oder durch von ihm beauftragte Dritte) stellt die erforderlichen Konfigurationsdateien bereit, welche der *Auftragnehmer* zur Einbindung des Druckgerätes in seine Printlösung benötigt. Nach der erfolgreichen Integration des Druckgerätes in die Printlösung des *Auftragnehmers* und nach Abschluss der Gesamtkonfiguration (z.B. Anlage der Printqueue, Aufspielen von Software) durch den *Auftragnehmer* erhält der *Auftraggeber* darüber automatisiert eine Bestätigung.

Der Serviceschnitt verändert sich während der Vertragslaufzeit. Ab 01/2029 wird der Arbeitsplatzdruckservice vollständig durch den *Auftragnehmer* erbracht, inklusive der vollständigen Konfiguration der MFP. Dies umfasst:

- Aufnahme der MFP ins Netz, soweit eine initiale Remotekonfiguration dies erfordert
- Aufspielen der notwendigen Firmware, Sicherheitstoken und Sicherheitseinstellungen und sonstigen mit dem *Auftraggeber* abgestimmten Konfigurationseinstellungen
- Installation von Software, die auf den MFP zur Umsetzung der vereinbarten Funktionalität benötigt wird (z.B. ein Client für das vertrauliche Follow Me-Drucken)
- nach erfolgreicher Konfiguration Übernahme der konfigurierten MFP in das Arbeitsplatz-Umfeld des *Auftraggebers*
- Benachrichtigung des *Auftraggebers* zum erfolgreichen Abschluss der Konfiguration.

Die folgenden beiden Tabellen verdeutlichen die Verlagerung der Aufgaben und Verantwortlichkeiten ab 2029:

10.5.1.1 Aufgabenverteilung bis 2028

Beschreibung	***Auftraggeber* (oder beauftragter Dritter)**	***Auftragnehmer***
Drucker Hardware	R	
Bereitstellung Daten	R	I
Netzintegration (Konfiguration DHCP, NAC-Verwaltung,...)	I	R
Vorbereitung automatisches Anlageverfahren	I	R
Konfiguration und Funktionstest	R	
Prestaging	R	
Security Konfiguration	R	
Mandantenspezifische Konfiguration	R	
Integration in backend		R
Erweiterter Zertifikatsprozess	R	
Mac Adresse im NAC löschen		R

Tabelle 6: Arbeitsplatzdruck Aufgabenverteilung I

10.5.1.2 Aufgabenverteilung ab 2029

Beschreibung	***Auftraggeber* (oder beauftragter Dritter)**	***Auftragnehmer***
Drucker Hardware	R	

Bereitstellung Daten	R	I
Netzintegration (Konfiguration DHCP., NAC-Verwaltung,...)	I	R
Vorbereitung automatisches Anlageverfahren	I	R
Konfiguration & techn. Funktionstest	I	R
Prestaging	I	R
Security Konfiguration	I,C	R
Mandantenspezifische Konfiguration	I,C	R
Integration in backend		R
Erweiterter Zertifikatsprozess	I,C	R
Mac Adresse im NAC löschen	I	R, sofern noch erforderlich

Tabelle 7: Arbeitsplatzdruck Aufgabenverteilung II

Ausprägung	Beschreibung
R = Responsible	Die jeweilige Partei ist für die einwandfreie Durchführung einer Leistung in vollem Umfang verantwortlich.
S = Sign-Off	Die jeweilige Partei, die die Ausführung einer Leistung freigibt. Dies impliziert, dass die jeweils andere Partei Informationen bereitstellen muss, die eine Freigabe ermöglichen.
C = Consulted	Die jeweilige Partei, die von der anderen Partei in Bezug auf Stellungnahmen oder beratend einzubinden ist. (2-Wege Kommunikation).
I = Informed	Die jeweilige Partei, die von der jeweils anderen Partei in Bezug auf die Leistung entsprechend zu informieren ist. (1-Weg Kommunikation).

Tabelle 8: RACI Matrix

Verwendet der *Auftragnehmer* zertifikatbasierte Verfahren zur Einbindung der MFP/ Drucker in den Arbeitsplatzdruckservice oder allgemeiner in die Arbeitsplatzinfrastruktur, so ist hierfür die PKI des *Auftraggebers* zu verwenden.

10.5.1.3 Zertifizierungen

Um das Zusammenspiel der in diesem LS geforderten zentralen Services für den Arbeitsplatzdruck zwischen den Geräten des *Auftraggebers* und der Infrastruktur des *Auftragnehmers* sicherzustellen, zertifiziert der *Auftragnehmer* die MFP-Hardware (inkl. Firmware) und Druckertreiber durch entsprechende Prüfungen und passt bei Bedarf die Konfigurationsdaten für Drucker und Treiber an. Erst danach werden die MFP in den Warenkorb des *Auftraggebers* und die Bestellprozesse aufgenommen.

Die Zertifizierung der Geräte und Treiber hat dabei in einer nicht produktiven Umgebung so zu erfolgen, dass die produktive Nutzung des Arbeitsplatzdruckes im Geschäftsbetrieb des *Auftraggebers* nicht beeinflusst wird. Der Ausdruck “nicht produktiv” meint an dieser Stelle, dass diese Umgebung für den regulären krankenkassenfachlichen Geschäftsbetrieb des *Auftraggebers* nicht erreichbar ist.

Der *Auftragnehmer* stellt dies durch geeignete Maßnahmen sicher (z.B. durch separate Umgebungen oder das „Auskoppeln“ von Geräten aus der produktiven Nutzung). Diese Umgebung muss auch als Testumgebung verwendbar sein, um Änderungen an der Software oder der Konfiguration oder den Bereitstellungsprozessen zertifizierter MFP vor einer Produktivsetzung gegen die technologischen Anforderungen überprüfen zu können. Die genaue Ausgestaltung dieser Umgebung ist in der Transitionsphase zwischen *Auftraggeber* und *Auftragnehmer* festzulegen. Für die Umgebung erforderliche MFP und Clients stellt der *Auftraggeber*, die jeweils notwendige Konfiguration erfolgt durch den *Auftragnehmer*.

Analog zu den Phasen des Rollouts bei Office Arbeitsplätzen ist auch beim Ausrollen von Änderungen an den MFP (neue Hardware-Modelle, Firmwareänderungen, Security-Patches, Konfigurationsänderungen etc.) eine Preprod-Phase mit einer beschränkten (<=20) Anzahl von MFP vorzusehen.

Es ist vom *Auftragnehmer* sicherzustellen, dass im Falle von erforderlichen Wartungsarbeiten (z.B. Treiberupdate) die Funktionalität des Service nicht beeinträchtigt wird.

10.5.1.4 Schnittstelle zum Output Management des Auftraggebers

Der *Auftraggeber* betreibt eine eigene Output Management Lösung, die Drucke sowohl zum Arbeitsplatzdruck wie auch zu anderen Druckdiensten leitet. Zum Zeitpunkt der Ausschreibung ist dafür Isis Papyrus im Einsatz.

Diese Lösung des *Auftraggebers* nutzt teilweise die Leistungen des *Auftragnehmers* zur Erzeugung von Druckoutput am Arbeitsplatz (z.B. der Transport eines gerenderten Druckauftrags an einen im Userkontext definierten Windows Standarddrucker). Im Rahmen des Druckprozesses werden Parameter für den Ausdruck aus einer applikationsspezifischen Vorlage gezogen. Die entsprechende Erfüllung der Parametrisierung (z.B. Schachtsteuerung; erste Seite Logopapier, folgende auf Normalpapier) muss über alle Druckgeräte sichergestellt sein. Sofern einem Anwender in einer Umgebung mehr als ein Druckobjekt zur Verfügung steht, muss der vom Anwender geänderte Windows Standarddrucker zur Laufzeit der betroffenen Drucklösung mitgeteilt werden.

Der *Auftragnehmer* verantwortet die korrekte Funktion seiner Leistungen im Zusammenwirken mit obiger Lösung des *Auftraggebers*. Die notwendigen Schnittstellen werden in Abstimmung zwischen *Auftraggeber* und *Auftragnehmer* definiert und umgesetzt.

Der *Auftragnehmer* stellt sicher, dass im Falle der Nichterreichbarkeit eines Dienstes oder Gerätes keine Druckaufträge verloren gehen.

10.5.1.5 Betriebsumgebung

Grundsätzlich sind die verschiedenen Umgebungen (z.B. Produktion, Test, Entwicklung o.ä.) mindestens auf logischer Ebene auf Basis der jeweils gegebenen technischen Möglichkeiten zu trennen. Die Trennung hat jeweils so zu erfolgen, dass eine gegenseitige Beeinflussung der Umgebungen in Bezug auf Integrität, Vertraulichkeit, Verfügbarkeit und Performance ausgeschlossen ist.

Die Umgebungstrennung ist auf logischer Ebene mindestens für die Produktionsumgebung und die Testumgebung vorzusehen.

Sollten mandantenfähige Systeme eingesetzt werden, müssen die Vorgaben aus **02-09-03 AVV-TOMs Informationssicherheit** - Kapitel 7.1 eingehalten werden.

Administrative Aufgaben, die die Umgebungstrennung bzw. Mandantentrennung berühren, sind mit fortgeschrittenen Sicherheitsmaßnahmen (**02-09-03 AVV-TOMs Informationssicherheit**) –

insbesondere starken Authentifizierungsmechanismen – vorzunehmen. Bzgl. Changes in diesem Umfeld ist unbedingt der Change-Management Prozess (siehe **02-04 Prozessrichtlinien**) einzuhalten.

Sollte für einen Service eine Verletzung der vorgenannten Anforderungen festgestellt werden, wird der *Auftragnehmer* für diesen Service ohne Mehrkosten (Initial und Betrieb) die Trennung so anpassen, dass die Anforderungen erfüllt werden.

10.5.2 Serviceleistungen zum Arbeitsplatzdruck

Im Folgenden sind insbesondere die für den IT-Service notwendigen Einzelleistungen, die durch den *Auftragnehmer* zu erbringen sind, beschrieben. Zur Strukturierung sind diese den verschiedenen ITIL Disziplinen zugeordnet, gelten aber unabhängig von dieser Zuordnung.

10.5.2.1 Übergreifende Serviceleistungen

Generelle Relevanz für den Lifecycle von IT-Services.

Der *Auftragnehmer* erbringt dabei folgende Leistungen:

- Sicherstellen der korrekten Funktion im Zusammenwirken mit Druck-, Fax- und Scanlösungen und OMS (Isis Papyrus) des *Auftraggebers*
- Definition der notwendigen Schnittstellen im Zusammenwirken mit Druck-, Fax- und Scanlösungen und OMS (Isis Papyrus) des *Auftraggebers*
- Implementierung und Betrieb der notwendigen Schnittstellen im Zusammenwirken mit den Druck-, Fax- und Scanlösungen und OMS (Isis Papyrus) des *Auftraggebers*
- Erstellung und Pflege erforderlicher Dokumentation, mindestens aber Feinkonzepte, Betriebshandbücher, die für die MFP gewählten Konfigurationsparameter, eine detaillierte Beschreibung der Schnittstellen zu Umsystemen, insbesondere OMS und FAX, sowie eine Beschreibung der Abhängigkeiten von den Dienstleistungen Dritter.

10.5.3 Service Design

Entwicklung von IT-Services auf Basis konkreter Anforderungen sowie Änderungen und / oder Verbesserungen bereits vorhandener IT-Services. Der *Auftragnehmer* erbringt dabei folgende Leistungen:

- Der *Auftragnehmer* stimmt die benötigten Informationen zur Bereitstellung des Service mit dem *Auftraggeber* ab.
- Der *Auftragnehmer* stimmt die benötigten Informationen zur Durchführung von Zertifizierungen mit dem *Auftraggeber* ab.
- Der *Auftragnehmer* konzipiert den Zertifizierungsprozess auf Basis der Richtlinien des *Auftraggebers*.
- Der *Auftragnehmer* konzipiert die Zertifizierungsumgebung auf Basis der realen Systemumgebungen
- Der *Auftraggeber* definiert die Abnahmekriterien für die Serviceprodukte zur Übergabe in den Betrieb.

10.5.4 Service Operation

Der *Auftragnehmer* stellt die effektive und effiziente Erbringung von IT-Services von der Erfüllung von Anwender-Anfragen über die Erarbeitung von Problemlösungen bis hin zur Erbringung von Betriebsaufgaben im Tagesgeschäft sicher. Dabei erbringt der *Auftragnehmer* folgende Leistungen:

- Vollständiger Betrieb des IT-Service, inkl. der seitens des *Auftraggebers* oder seitens Dritter bereitgestellten MFP inkl. der Schnittstellen zu Umsystemen
- Regelmäßige Sicherung relevanter Daten insbesondere Konfigurationsdaten und Warteschlangen
- Bereitstellung und Customizing des zentralen Printer Mappings
- Unterstützung der Druckereinrichtung durch automatisierte Bereitstellung von Konfigurationsdaten für den Anschluss und Aufnahme der Geräte in die Infrastruktur (IP Adressmanagement, Druckwarteschlange etc.)
- Vollständige Druckereinrichtung und Aufnahme der Geräte in die Infrastruktur
- Durchführung von Drucker- und Treiberzertifizierungen in Prüfumgebungen; hierbei ist darauf zu achten, dass die Produktivsysteme durch den Prüfbetrieb nicht beeinflusst werden. Anpassung der für MFP und Treiber erforderlichen Konfiguration/Parametrisierung.
- Durchführung von Maßnahmen nach erfolgter Abstimmung mit dem Auftraggeber zur Gewährleistung eines vom jeweiligen Hersteller gewarteten Versions- bzw. Releasestandes für alle Komponenten des Serviceproduktes
- Durchführung von Maßnahmen nach erfolgter Abstimmung mit dem Auftraggeber zur Gewährleistung eines vom jeweiligen Hersteller gewarteten Versions- bzw. Releasestandes für alle Komponenten des Serviceproduktes
- Administration von Security Parametern gemäß den Anforderungen des *Auftraggebers* und der Best Practices des *Auftragnehmers*
- Konfiguration von Serviceparametern zur Aufrechterhaltung und Optimierung der Servicequalität
- Management der Nutzerberechtigungen für Authentifikation über geeignete Verfahren
- Konfiguration von Standardparametern für alle Komponenten der Serviceprodukte
- Konfiguration von Endgeräten (MFP) sowie angeschlossener Peripheriegeräte (z.B. Kartenleser) zur korrekten Funktion der Printlösung
- Durchführung des Lifecycle Managements (Erstellen, Ändern, Löschen) für alle benötigten Komponenten des Service
- Status Updates an Service Desks von *Auftraggeber*, *Auftragnehmer* und definierten Dritten
- Unterstützung des Service Desks von *Auftraggeber*, *Auftragnehmer* und definierten Dritten

11 Kommunikation & Kollaboration

Die Services im Bereich Unified Communication and Collaboration (UCC) umfassen eine ganzheitliche Kommunikations- und Kollaborationsinfrastruktur, die speziell darauf ausgerichtet ist, den Austausch und die Zusammenarbeit intern beim *Auftraggeber,* aber auch nach extern, effizient, performant und sicher zu gestalten.

Die UCC-Services kombinieren wesentliche Bausteine der UCC, darunter File Services, Microsoft Exchange für die E-Mail-Kommunikation. Im Folgenden wird näher auf die einzelnen Services eingegangen.

11.1 File Services

Der *Auftragnehmer* stellt den Mitarbeitern des *Auftraggebers* verschiedene Fileshares und File Services innerhalb ihrer Arbeitsumgebung (sowohl im virtuellen Arbeitsplatz als auch auf den

klassischen Windows-Fat-Clients) über lokale Zugriffsmöglichkeiten zur Verfügung. Die Fileshares betreffen aktuell folgende Bereiche:

- Nutzerprofile und Home-Laufwerke
- Gruppen-Laufwerke im Rahmen der Organisationsstrukturen des *Auftragnehmers*, mit Berechtigungssteuerung über IAM (Identity und Access Management) des *Auftraggebers* gemäß Vorgaben in **02-02 Technologiegrundsätze**

Über die Fileshares der Gruppen-Laufwerke werden den Mitarbeitern Unternehmensdaten zur Verfügung gestellt, die in großen Teilen als Sozialdaten und Betriebsgeheimnisse besonders schützenswert sind und gemäß der (Anlage **02-09-03 AVV-TOMs Informationssicherheit**) verschlüsselt sind.

Der *Auftraggeber* hat Tools und Prozesse für die Berechtigungsverwaltung im Einsatz. Diese müssen durch den *Auftragnehmer* implementiert und angewendet werden. Der *Auftragnehmer* übernimmt die folgenden Aufgaben:

- Der *Auftragnehmer* stellt initial mindestens eine Speicherkapazität von 250 TB zur Verfügung.
- Bereitstellung neuer Gruppen- oder Projektshares und initiale Berechtigung der Administratoren des *Auftraggebers* bzw. administrativen Gruppen
- Zentrale Rechtevergabe und -korrektur, soweit dies nicht über Auftraggebersysteme (z.B. IAM) oder Self-Services möglich ist, wie zum Beispiel übergreifende Distributed File System (DFS)-Shares
- Löschen und Reorganisieren von Gruppen- oder Projektshares einschließlich der Berechtigungen im Auftrag und in Zusammenarbeit mit dem *Auftraggeber*
- Managen von Profil- und Home-Laufwerken im Kontext Anlage und Beenden von Nutzern des *Auftraggebers*
- Kurzfristige Bereitstellung von Zugriffen und/oder Datenexporten an berechtigte Personen im Kontext doloser Handlungen über separaten und eingeschränkt sichtbaren Service-Request
- Bereitstellung von Self-Services für die Mitarbeiter
    - Tool zur Rechteverwaltung durch Administratoren mit Änderungsverfolgung für Revisionszwecke und folgenden Basisrechten (Lesen, Schreiben, Vollzugriff = Administrator)
    - Abfrage/Übersicht von Administratoren im Rahmen der dezentralen Rechteverwaltung
    - Lokale Wiederherstellung älterer Datenversionen in zeitlich begrenztem Umfang (lokale Änderungshistorie)

11.2 E-Mail-Service

11.2.1 Status-Quo

Der aktuelle E-Mail-Service des *Auftraggebers* umfasst ca. 21.000 Postfächer und basiert auf Microsoft Exchange 2016 und Outlook 2016. Im Einsatz sind 10 Exchange Server und 2 Admin-Server mit ca. 19.000 GB Storage-Bedarf.

Diese Exchange Umgebung wird On-Premise in einer Hybrid-Konfiguration mit Exchange-Online betrieben. Exchange-Online wird für die Termin-Synchronisierung und Kalenderinformationen verwendet. Zusätzlich zu dieser Produktivumgebung wird eine physikalisch getrennte Non-Prod-

Umgebung mit 2 Exchange-Servern betrieben.

Die initiale Anlage von User-Postfächern erfolgt automatisiert über das IAM. Die Mailbox Größe ist initial auf 2 GB begrenzt. Eine Erweiterung kann im Self-Service via IAM beantragt werden.

Zur Reduzierung der Postfachspeichergröße wird derzeit die Lösung Veritas Enterprise Vault (On-Premise) eingesetzt (ca. 17.000 GB Archiv-Storage-Bedarf). Aktuell wird außerdem die Mail Security Lösung „BISS Mail Security“ für ca. 21.000 Postfächer mit ca. 6.500 E-Mail Encryption Gateway Lizenzen eingesetzt.

11.2.2 Aktuelle Vorhaben

Im Jahr 2025 ist die Migration der Postfächer zu Exchange-Online im Tenant des *Auftraggebers* geplant. Mit der Migration nach Exchange-Online wird die Postfachgröße für alle User auf 50 GB erweitert. Eine Erweiterung auf 100 GB ist möglich. Die Verwendung der Exchange-Online Archivierungslösung ist ebenfalls geplant. In diesem Zusammenhang wird der Einsatz der aktuell verwendeten Mail Security Lösung (Mail Security Gateway) mit Exchange-Online geprüft.

Ebenfalls wird im Rahmen des Migrationsprojekts geprüft, ob Mitarbeiter- und Gruppen-Postfächer aufgrund von regulatorischen Anforderungen weiterhin On-Premises bereitgestellt werden müssen. Bei einer vollständigen Migration aller Postfächer nach Exchange Online wird der Einsatz eines On-Premises “Blind Relays” evaluiert. Daraus resultieren die Zielgröße und -architektur der zukünftigen On-Premises Exchange-Umgebung.

11.2.3 Auftragnehmerleistungen

Der *Auftragnehmer* verantwortet die initiale Konfiguration, den Betrieb, die Wartung und Pflege der On-Premises Infrastruktur, der Exchange Online-Instanz im Tenant des *Auftraggebers*, der Postfächer sowie der Hybridkonfiguration.

Ferner übernimmt der *Auftragnehmer* die über das ITSM-Tool des *Auftraggebers* eingestellten Service Requests und die Bearbeitung von 2nd- und 3rd-Level-Incidents im Kontext des Mail Service.

Folgende Service-Requests sollen durch den *Auftragnehmer* übernommen werden, sofern die Bereitstellung über den OneIdentity Self Service nicht implementiert wurde oder in Einzelfällen Fehler aufweist:

- Anpassung der Aufbewahrungsrichtlinie(n)
- Datenbank-Wiederherstellung
- Disclaimer-Konfiguration & -Anpassung
- Bereitstellung von Nachrichtenverfolgungsprotokollen
- Anpassung der Organisationskonfiguration
- Postfach-Wiederherstellung
- Bereitstellung der Revisionssicherung (als .pst-File, bereitzustellen an einem durch den *Auftraggeber* zu definierenden Speicherort [z. B. SharePoint Online-Bibliothek])
- Konfiguration und Anpassung von Transportagenten und -konnektoren
- Bereitstellung von Überwachungsprotokollen (bereitzustellen an einem durch den *Auftraggeber* zu definierenden Speicherort [z. B. SharePoint Online-Bibliothek])
- Wiederherstellung öffentlicher Ordner
- Prüfung / Konfiguration von Postfachberechtigungen
- Prüfung / Einrichtung / Änderung von Vertretungsregelungen
- Erstellung, Modifikation oder Löschung von Exchange Komponenten wie z. B. Mail-

Security (Black- oder Whitelisting etc.)
- Einrichtung und Konfiguration und Pflege von Sonder-Postfächern (z. B. Personalrat, Schwerbehindertenvertretung oder Datenschutz, sofern nicht über ONE IDENTITY Self Service abgedeckt)

Der Leistungsumfang beinhaltet die Durchführung von Änderungen an Exchange Komponenten (bzw. deren Konfiguration) sowie Änderungen am Mail-Flow und Mail-Security.

Zusätzlich informiert der *Auftragnehmer* den Service Owner des *Auftraggebers* proaktiv über notwendige und optionale Updates. Dabei evaluiert der *Auftragnehmer* die durch Änderungen resultierenden Auswirkungen, inklusive möglicher Risiken, und stimmt diese mit dem Service Owner des *Auftraggebers* ab, um vor Implementierung der Änderungen dessen Freigabe einzuholen (gem. Change-Management-Vorgaben des *Auftraggebers*, wie in Anhang **02-04 Prozessrichtlinien** beschrieben).

Dem *Auftragnehmer* werden die notwendigen Rollen und Berechtigungen im Tenant des *Auftraggebers* zugewiesen.

12 Remote Support Management

Der *Auftragnehmer* stellt eine datenschutzkonforme und sichere (mindestens zu den Bausteinen BSI IT-Grundschutzes oder vergleichbaren Standards konforme) Remote-Support-Lösung für alle virtuellen und physischen Windows-Clients des *Auftraggebers* über das interne Netz bereit. Der *Auftragnehmer* stellt sicher, dass die Lösung dem *Auftragnehmer*, *Auftraggeber* und Dritten (z.B. UHD) zur Verfügung steht.

Ein Remote-Zugriff auf interne Geräte des *Auftraggebers* ist nur im Ausnahmefall möglich und folgenden Einschränkungen unterworfen:

- Der *Auftragnehmer* verpflichtet sich, Remote-Aktivitäten nur auf Weisung des *Auftraggebers* von hierzu autorisierten Mitarbeitern ordnungsgemäß durchführen zu lassen. Diese Mitarbeiter teilt der *Auftragnehmer* dem *Auftraggeber* mit.
- Der Aufbau der Remote-Verbindung darf nur über den eingerichteten VPN-Zugang des *Auftraggebers* erfolgen. Die Fernwartungsverbindung wird im Havariefall ausschließlich vom *Auftraggeber* nur zeitlich limitiert aktiviert. Die Remote-Aktivitäten werden protokolliert.
- Der *Auftraggeber* räumt dem *Auftragnehmer* nur die Zugriffsrechte ein, die dieser zur Durchführung der Remote-Sitzung tatsächlich benötigt. Der *Auftragnehmer* darf von den ihm eingeräumten Zugriffsrechten nur in dem für die Durchführung der Remote-Arbeiten unerlässlich notwendigen Umfang Gebrauch machen.
- Der *Auftragnehmer* darf personenbezogene Daten im Wege eines Filetransfers oder Downloads für Zwecke der Fehleranalyse und -behebung nur dann vom DV-System des *Auftraggebers* abziehen und auf sein eigenes kopieren, wenn er dafür zuvor die schriftliche Erlaubnis des Auftraggebers eingeholt hat. Notwendige Datenübertragungen zu Zwecken der Wartung müssen in hinreichend verschlüsselter Form erfolgen.
- Der *Auftraggeber* ist berechtigt, die Remote-Sitzung von einem Kontrollbildschirm aus zu verfolgen und jederzeit abzubrechen. Soweit der *Auftraggeber* daran mitwirken muss, gewährleistet er, dass dies möglich ist. Die Unterbrechung kann auch erfolgen, wenn ein Remote-Zugriff mit nicht vereinbarten Hard- und/oder Softwarekomponenten festgestellt wird.

- Der *Auftragnehmer* muss personenbezogene Daten, die er bei der Remote-Sitzung erhalten hat, unverzüglich löschen oder dem *Auftraggeber* zurückgeben, wenn sie für die Durchführung der Remote-Arbeiten nicht mehr erforderlich sind.

13 Beratungsleistungen

13.1 Leistungsumfang

Der *Auftragnehmer* muss über die Vertragslaufzeit die im Dokument **01-07 Skillprofile** beschriebenen Skills mit den entsprechenden Qualifikationen vorhalten und im Falle eines Abrufs zur Verfügung stellen. Der Abruf von Beratungs- und Entwicklungsleistungen, welche über die abgeschlossene Transitionsphase hinausgehen (Abrufbudget), erfolgt in Einzelabrufen, die sich in der Regel auf ein konkretes Projekt oder Vorhaben bzw. eine definierte Beratungstätigkeit beziehen (siehe Dokument **02-05 Projektgrundsätze**). Der *Auftraggeber* wird im Sinne einer gemeinsamen Planung den *Auftragnehmer* frühzeitig über seine Planungen und den geschätzten Bedarf in einer Vorabinformation unterrichten.

Mit dieser Vergabe sollen Beratungs- und Entwicklungsleistungen des *Auftragnehmers* nach Abschluss der Transitionsphase in dem im **01-06 Leistungsverzeichnis** hinterlegten geschätzten Umfang beschafft werden. Dieser Ressourcenbedarf ist ein geschätzter Wert und stellt eine Orientierungsgröße für die Angebotsabgabe dar. Für die geschätzten Bedarfe besteht keine Abnahmeverpflichtung, weder je definiertem Skillprofil noch insgesamt.

Der *Auftraggeber* plant, die Skillprofile beispielhaft für folgende Themenfelder zu beauftragen:

- Umstieg auf Microsoft Intune
- Professionalisierung und Nutzung weiterer Services aus dem Leistungsspektrum M365
- Effizienzsteigerung durch Nutzung von Automatisierung / Automatisierungstechnologien im Betrieb und Service
- Fileservice Migration zu Cloud Service
- Umstieg Hybrid Windows Client zu Entra Client

Für weitere Regelung zur Vergütung der Skillprofile wird auf die Anlage **02-08 Vergütung** Ziff. 4 verwiesen.