

Vergabeunterlage B

Leistungsbeschreibung

Cloud-Leistungen

30.09.2026

dbhn  dachgesellschaft
bauvorhaben
hochschulmedizin
niedersachsen

Inhaltsverzeichnis

1. Ausgangssituation	5
1.1. Auftraggeber und Ausgangssituation.....	5
1.2. Zielsetzung	6
1.3. Vergabegegenstand und Leistungsumfang	8
2. Kriterien	9
2.1. Art der Cloud.....	9
2.1.1. Souveräne Managed Cloud	9
2.1.2. Betrieb der Infrastruktur	9
2.1.3. Compute-Ressourcen.....	10
2.1.4. Storage-Ressourcen	10
2.1.5. Netzwerk-Infrastruktur	10
2.2. Managed Cloud Services (MCS)*	11
2.2.1. Ansprechpartner / Mitwirkungspflichten	11
2.2.2. Zugangsverwaltung / Administration.....	11
2.2.3. Service Desk / Hotline	12
2.2.4. Request Fulfillment	13
2.2.5. Kapazitätsmanagement und Monitoring	13
2.2.6. Automatisierung von Routineaufgaben	14
2.2.7. Incident- und Problemmanagement.....	15
2.2.8. Change Management	15
2.2.9. Eskalationsverfahren	16
2.2.10. Release- und Patchmanagement.....	16
2.2.11. Backup & Restore	17
2.3. Leistungsort.....	18
2.4. Georedundanz.....	18
2.5. Übergabepunkt.....	18
2.6. Bereitstellungszeitpunkt.....	19

2.7.	Nutzer	19
2.8.	Nutzerkreis.....	20
2.9.	Nutzungsort.....	21
2.10.	Identitäts- und Berechtigungsmanagement (IDM)	21
2.11.	Endgeräte.....	21
2.12.	Speicher-Größe (für Speicherung von Auftraggeberdaten).....	22
2.12.1.	SAN je VM.....	22
2.12.2.	NAS	22
2.13.	Art der Anbindung.....	22
2.13.1.	Anbindung der Managed Cloud	23
2.13.2.	Remote-Access / VPN-Einwahl	23
2.14.	Bandbreite der Anbindung des Auftragnehmers	23
2.15.	Datensicherung*.....	23
2.15.1.	Backup-Verfahren.....	24
2.15.2.	Backup-Intervall	24
2.15.3.	Aufbewahrungsfristen	24
2.15.4.	Backup-Speicherort.....	25
2.15.5.	Restore	25
2.15.6.	Wiederherstellungstests	25
2.15.7.	Verschlüsselung	25
2.16.	IT-Sicherheit.....	26
2.17.	Verfügbarkeit.....	27
2.18.	Gutschriften bei Nichtverfügbarkeit.....	27
2.19.	Reaktions- und Wiederherstellungszeiten	28
2.20.	Protokollierung.....	28
2.21.	Aktualisierung.....	29
2.22.	Reporting.....	29
2.23.	Mitwirkungsleistungen des Auftraggebers.....	30
3.	Bestandteile der Managed Cloud: Architektur und Infrastruktur	30

3.1.	Virtuelle Maschinen – Inbetriebnahme	30
3.2.	Storage	31
3.2.1.	SAN	31
3.2.2.	NAS	33
3.3.	RAM-Speichererweiterung	33
3.4.	Kommunikationssicherheit.....	33
4.	Erweiterung und Reduzierung der Leistung	34
5.	Dienstleistungen	34
5.1.	Überblick	34
5.2.	Einmalige Projekt-/Bereitstellungskosten.....	34
5.3.	Monatliche Betriebspauschalen	36
5.4.	Technische Beratung und Unterstützungsleitung auf Tagespauschalpreisbasis	37
6.	Service Level.....	37
6.1.	Verfügbarkeiten	37
6.2.	Priorisierung, Reaktions- und Wiederherstellungszeiten	38
6.3.	Service Level Management	39
6.4.	Gutschrift	40
7.	Dokumentation	40

1. Ausgangssituation

1.1. Auftraggeber und Ausgangssituation

Die Auftraggeber sind

- + die Dachgesellschaft Bauvorhaben Hochschulmedizin Niedersachsen mbH (DBHN), Andreaestraße 7, 30159 Hannover;
- + Die Hochschulmedizin Hannover Baugesellschaft mbH (HBG), Podbielskistraße 386, 30659 Hannover;
- + Die Baugesellschaft Universitätsmedizin Göttingen mbH (BauG UMG), Robert-Koch-Straße 34, 37075 Göttingen.

Nachfolgend gemeinschaftlich als „Gesamtauftraggeber“ bezeichnet.

Das Land Niedersachsen hat zum Zwecke der Bündelung der im Zusammenhang mit den Bauvorhaben Neubau-, Umbau- und Sanierung der UMG und der MHH stehenden Aufgaben der Landesverwaltung eine Gesellschaft, die DBHN, gegründet. Die Aufgabe der DBHN ist es, im Interesse des Landes Niedersachsen eine zentrale Steuerung bei der Sanierung der Krankenversorgung sowie bei Baumaßnahmen im Bereich Forschung und Lehre der Medizinischen Hochschule Hannover und der Universitätsmedizin der Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts zu gewährleisten. Dies umfasst insbesondere die Wahrnehmung von Steuerungs-, Prüfungs-, Kommunikations- und Kontrolltätigkeiten für das Land Niedersachsen einschließlich der Fortentwicklung bestehender Medizin- und Baustandards. Sie hält zu diesem Zweck Anteile an den beiden Baugesellschaften der Hochschulkliniken, die an den jeweiligen Hochschulklinikstandorten ansässig sind.

Die beiden Baugesellschaften, HBG und BauG UMG, übernehmen nach dem System der zentralen Steuerung die Bauherrenaufgaben bei den jeweiligen klinischen Baumaßnahmen und sind somit für die gesamten Planungs- und Bauprozesse bis hin zur Übergabe der Neubauten verantwortlich.

Zur Wahrnehmung der Aufgaben der Auftraggeber werden verschiedene Fachanwendungen genutzt, die heute teilweise als SaaS-Lösung, teilweise On-Premise- und teilweise in einer Public Cloud betrieben werden.

Die erarbeitete Cloud-Lösung dient den einzelnen Unternehmen, als zentrale Plattform für die Arbeitsprozesse der Auftraggeber sowie die Zusammenarbeit mit den beteiligten Partnerunternehmen.

1.2. Zielsetzung

MOTIVATION FÜR DIE MIGRATION IN EINE MANAGED CLOUD-INFRASTRUKTUR

Der Gesamtauftraggeber verfolgt das Ziel, ausgewählte Windows-Server-Anwendungen schrittweise aus dem bestehenden unternehmenseigenen Rechenzentrum in eine Managed Cloud zu überführen. Zusätzlich sollen neue Anwendungen auf der Managed Cloud Infrastruktur betrieben werden. Ziel dieser Strategie ist es, die bestehende Infrastruktur nachhaltig zu entlasten und gleichzeitig die Anforderungen an Informationssicherheit, Hochverfügbarkeit, Skalierbarkeit und zukünftiges Unternehmenswachstum zu erfüllen.

Die Managed Cloud Infrastruktur ist so auszulegen, dass sie den Betrieb der DBHN sowie der beiden Gesellschaften BauG UMG und HGB unterstützt und zukünftige Erweiterungen ohne grundlegende Architekturänderungen ermöglicht. Hierzu ist eine souveräne Managed Cloud bereitzustellen, deren Betrieb vollständig durch den Auftragnehmer erfolgt.

Die Migration erfolgt stufenweise, um Risiken für den laufenden Geschäftsbetrieb zu minimieren und eine kontrollierte Inbetriebnahme der einzelnen Systeme sicherzustellen.

Aktuell sind die nachfolgenden Phasen für die Nutzung der Cloud angedacht. Abrufe erfolgen grundsätzlich anhand der tatsächlichen Bedarfe und Entscheidungen.

PHASE 1 – AUFBAU DER MANAGED CLOUD-BASISINFRASTRUKTUR

Im ersten Projektschritt ist die Managed Cloud bereitzustellen und in die bestehende IT-Infrastruktur des Auftraggebers zu integrieren. Hierzu gehört die Anbindung an das bestehende Active Directory der Auftraggeber durch den Aufbau eines Domänencontrollers innerhalb einer virtuellen Maschine in der Managed Cloud.

PHASE 2 – EINFÜHRUNG DER CONTROLLING-PLATTFORM

Zu diesem Zeitpunkt müssen sämtliche Netzwerkverbindungen zwischen den Unternehmensstandorten und der Managed Cloud eingerichtet und betriebsbereit sein. Ebenso ist eine sichere Einwahlmöglichkeit für Home-Office-Arbeitsplätze bereitzustellen, sodass die Managed Cloud Infrastruktur unmittelbar produktiv genutzt werden kann.

Nach Bereitstellung der Basisinfrastruktur erfolgt die Installation / Einführung der neuen Controlling-Software innerhalb der Managed Cloud. Hierzu gehört die Installation der Software, die Einrichtung und das Customizing der Datenbank sowie die Anbindung der erforderlichen Datenquellen.

Insbesondere sind die Daten aus DATEV, den ELO-Systemen sowie der Projektmanagementsoftware iTWO zu integrieren. Gleichzeitig ist der produktive Zugriff sämtlicher berechtigten Anwender auf die neue Controlling-Plattform sicherzustellen.

Mit Abschluss der zweiten Projektphase werden von allen drei Gesellschaften ca. 60 Anwender auf verschiedene Systeme zugreifen.

PHASE 3 – MIGRATION WEITERER FACHANWENDUNGEN

Im nächsten Ausbauschnitt sollen verschiedene Fachanwendungen wie ELO Contract und ELO Invoice in die Managed Cloud migriert und dort produktiv betrieben werden.

Für jede produktive Anwendung soll eine eigenständige Testumgebung in verschiedenen VMs bereitgestellt werden, damit Softwareupdates, Konfigurationsänderungen und Funktionserweiterungen vor ihrer produktiven Einführung getestet werden können.

Neben dem Backup durch den Auftragnehmer soll ein Backup auf Basis von VEEAM Backup etabliert und vom Auftraggeber betrieben und verantwortet werden. Die Sicherungsdaten sollen in das bestehende Rechenzentrum des Auftraggebers übertragen und dort entsprechend den definierten Aufbewahrungs- und Archivierungsvorgaben langfristig vorgehalten werden.

PHASE 4 – ERWEITERUNG DER MANAGED CLOUD-INFRASTRUKTUR

Zur Unterstützung des weiteren Unternehmenswachstums ist die souveräne Managed Cloud so zu konzipieren, dass sie ohne grundlegende Architekturänderungen erweitert werden kann.

Voraussichtlich werden in Phase 4 weitere Applikationen in zusätzlichen VM installiert. Diese dienen der Migration der derzeit extern betriebenen Projektmanagementplattform (PKMS) in die Managed Cloud.

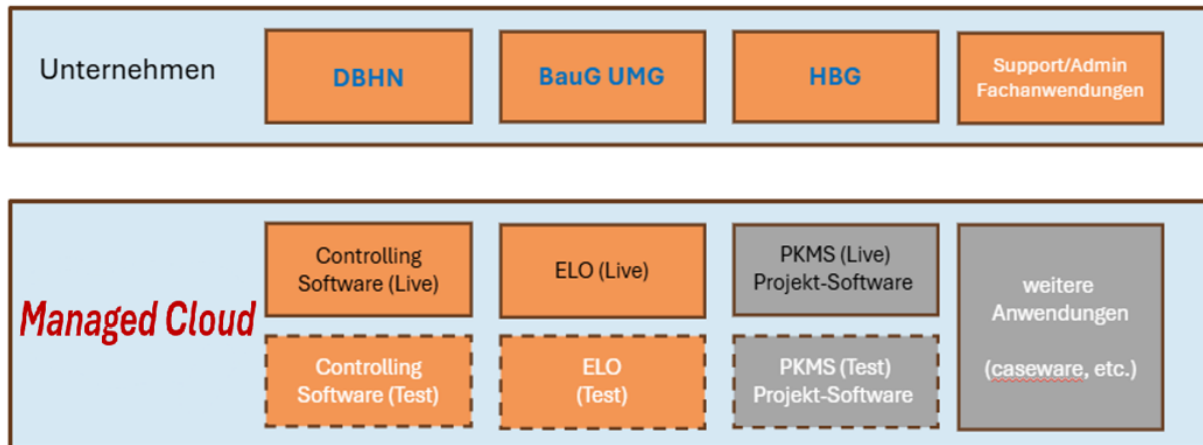
Mit der Inbetriebnahme dieser VM wird die Zahl der extern zugreifenden Anwender deutlich steigen. Es ist davon auszugehen, dass künftig 500 zusätzliche externe Projekt- und Bauleitungsmitarbeiter über gesicherte Remote-Zugänge auf die Managed Cloud Infrastruktur und die VM der PKMS zugreifen werden.

Aus diesem Grund sind Netzwerkarchitektur, VPN-Infrastruktur, Sicherheitskomponenten sowie die verfügbaren Ressourcen bereits bei der Erstimplementierung so zu planen, dass diese Erweiterung ohne grundlegende Änderungen der Architektur umgesetzt werden kann.

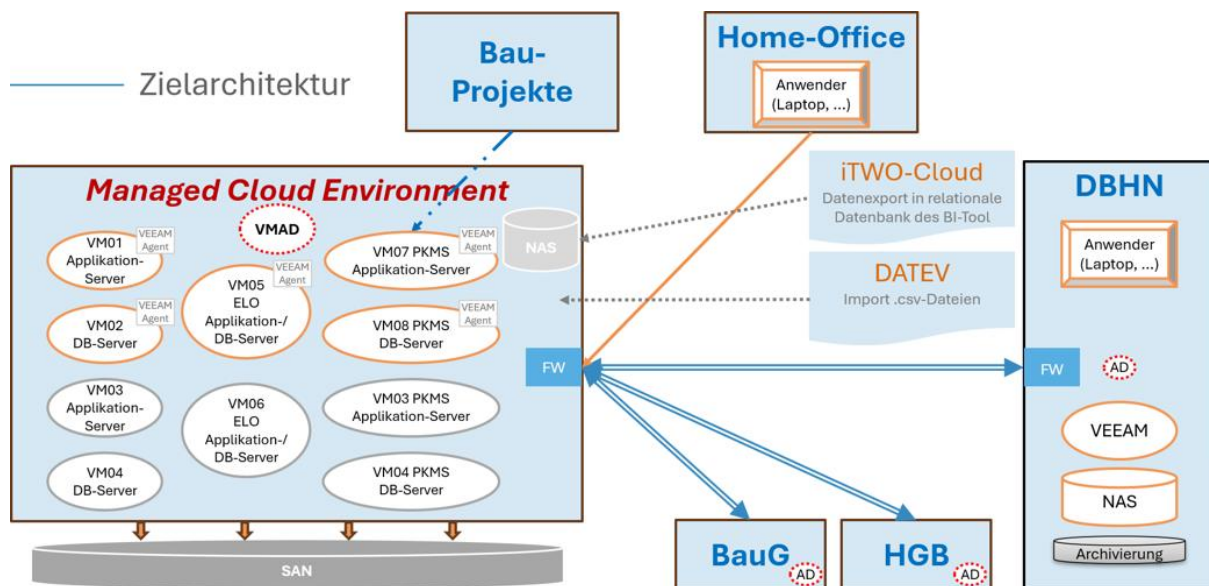
ZIELBILD

Die ausgeschriebene Managed Cloud bildet die zukünftige zentrale Betriebsplattform für die geschäftskritischen Anwendungen des Auftraggebers. Sie muss daher von Beginn an auf einen schrittweisen Ausbau ausgelegt sein und sowohl die Integration weiterer Anwendungen als auch die steigende Anzahl interner und externer Anwender unterstützen. Die Architektur ist unter Berücksichtigung hoher Anforderungen an Verfügbarkeit, Sicherheit, Skalierbarkeit und Wartbarkeit zukunftssicher auszulegen.

Schrittweise wird geplant die folgende Applikationslandschaft auf die souveräne Managed Cloud migriert:



Daraus ergibt sich folgende Einbettung in die DBHN-Systemlandschaft:



1.3. Vergabegegenstand und Leistungsumfang

Im Rahmen dieses Vergabeverfahrens wird eine **Managed Cloud** beschafft, auf die verschiedene bestehende und neue Fachanwendungen migriert und betrieben werden.

Ein wichtiger Bestandteil und Gegenstand dieses Vergabeverfahrens sind der Betrieb, die Betreuung und der Support der Managed Cloud.

2. Kriterien

Gegenstand dieser Ausschreibung ist die Bereitstellung, der Betrieb sowie die Wartung einer Managed Cloud.

Die nachfolgenden Kriterien wurden aus dem „EVB-IT Cloud – Kriterienkatalog für Cloudleistungen“ mit Stand 01.03.2026 entnommen. Ein separater Kriterienkatalog ist der Ausschreibung nicht beigelegt.

2.1. Art der Cloud

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.1 – Art der Cloud“ des EVB-IT Cloud Kriterienkatalogs.

2.1.1. Souveräne Managed Cloud

Mit der Ausschreibung fordert der Auftraggeber ein Angebot für eine Souveräne Managed Cloud.

Unter einer Souveräne Managed Cloud wird im Rahmen dieser Ausschreibung eine ausschließlich für den Auftraggeber bereitgestellte und betriebene Managed Cloud verstanden. Sämtliche für den Betrieb der Lösung erforderlichen Ressourcen (CPU-Cores, RAM, Storage) sind dem Auftraggeber exklusiv zugeordnet und dürfen nicht gemeinsam mit anderen Kunden genutzt werden. Es handelt sich um eine souveräne Umgebung für den Auftraggeber, welche im Rechenzentrum bzw. in den Rechenzentren des Auftragnehmers betrieben wird. Der Auftraggeber erwartet eine ausschließliche Nutzung der bereitgestellten Ressourcen, nicht der darunter liegenden Hardware (z. B. Server). Das Design und die Nutzung obliegt dem Auftragnehmer unter Berücksichtigung der gestellten Qualitätsanforderungen des Auftraggebers.

Die Bereitstellung erfolgt als Managed Cloud. Der Auftragnehmer übernimmt den vollständigen Betrieb, die Wartung, die Überwachung und den Support der Infrastruktur im Rechenzentrum.

2.1.2. Betrieb der Infrastruktur

Der Auftragnehmer ist für den vollständigen Betrieb der Managed Cloud-Infrastruktur verantwortlich. Hierzu gehören insbesondere:

- + Rechenzentrumsbetrieb
- + Stromversorgung und Klimatisierung
- + Physische Sicherheit
- + Netzwerk-Infrastruktur
- + Firewall-Systeme

- + Server-Hardware
- + Virtualisierungsplattform (Windows Server Data Center + Hyper-V oder VM-Ware)
- + Storage-Infrastruktur
- + Backup-Infrastruktur
- + Patch- und Wartungsmanagement der Infrastruktur
- + Störungsbeseitigung sowie Hardwareaustausch
- + Monitoring

Der Betrieb der auf der Managed Cloud Infrastruktur betriebenen Fachanwendungen (vgl. Zielbild in Kapitel 1.2) wird vom Auftraggeber bzw. weiteren Dienstleistern des Auftraggebers verantwortet. Ein Backup für die Daten der Fachanwendungen erfolgt jedoch auch durch den Auftragnehmer (vgl. Kapitel 2.2.11).

2.1.3. Compute-Ressourcen

Die Compute-Ressourcen müssen dem Auftraggeber zur Verfügung stehen.

Dies umfasst insbesondere:

- + Virtualisierungsplattform für den Betrieb von verschiedenen VMs (siehe 3.1 - Virtuelle Maschinen – Inbetriebnahme)
- + CPU - Cores (Kerne), Arbeitsspeicher (RAM)
- + keine Überbuchung (Overcommitment) der zugesicherten Ressourcen

Die zugesicherten Ressourcen müssen jederzeit vollständig verfügbar sein.

2.1.4. Storage-Ressourcen

Die Speicherinfrastruktur ist für den Auftraggeber bereitzustellen (siehe 3.1 - Virtuelle Maschinen – Inbetriebnahme und 3.2 - Storage).

Dies umfasst insbesondere:

- + SAN mit direktem Anschluss (z.B. über SAN-Switches) an die Hosts (Server)
- + Storage-Controller bzw. logisch der VM zugeordnete Controller
- + garantierte Performance hinsichtlich IOPS, Bandbreite und Latenz

Die produktiven Daten des Auftraggebers dürfen ausschließlich auf den vereinbarten Speicherressourcen abgelegt werden.

2.1.5. Netzwerk-Infrastruktur

Die Netzwerkkomponenten umfassen insbesondere:

- + Firewall-Instanzen
- + Firewall-Regelwerke
- + Netzwerksegmente
- + VLAN-/VXLAN-Strukturen
- + Load Balancer
- + VPN-Gateways

2.2. Managed Cloud Services (MCS)*

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.2 – Managed Cloud Services (MCS)“ des EVB-IT Cloud Kriterienkatalogs.

Der Auftragnehmer erbringt folgende ergänzende Leistungen (Managed Cloud Services*):

2.2.1. Ansprechpartner / Mitwirkungspflichten

Der Auftragnehmer benennt einen zentralen Ansprechpartner für den Auftraggeber. Er übernimmt auch die Regelkommunikation zum Supportteam und steuert die Umsetzung der Anforderungen des Auftraggebers.

Der Auftraggeber stellt Ansprechpartner und Anforderungen für die Managed Cloud Umgebung bereit.

2.2.2. Zugangsverwaltung / Administration

Der Auftragnehmer übernimmt die Administration der Managed Cloud Infrastruktur einschließlich der Benutzer- und Berechtigungsverwaltung auf Infrastruktur- und Managementebene. Hierzu gehören die Anlage, Änderung und Löschung administrativer Zugänge sowie die Verwaltung privilegierter Konten.

Der Auftragnehmer hat für sämtliche administrativen Tätigkeiten ab der Applikations- und Middleware-Schicht personenbezogene Administratorenkonten bereitzustellen. Dies gilt für Mitarbeitende des Auftraggebers, beauftragte Dienstleister des Auftraggebers sowie die Support-Mitarbeiter der eingesetzten Fachanwendungen.

Der Auftraggeber installiert und administriert die Anwendungen (z. B. AD, SQL-Server, ELO, BI/CPM, PKMS) sowie deren Konfiguration. Hierzu benötigen der Auftraggeber und von ihm beauftragte Dienstleister Administratorrechte innerhalb der virtuellen Maschinen.

Administrative Zugänge zum nativen Betriebssystem, zur Virtualisierungsplattform sowie zu den zugrunde liegenden Infrastrukturkomponenten sind hiervon ausdrücklich ausgenommen und verbleiben ausschließlich im Verantwortungsbereich des Auftragnehmers.

Jede Person, die administrative Berechtigungen erhält, muss über ein eigenes, eindeutig zugeordnetes Administratorkonto verfügen. Die gemeinsame Nutzung von Administratorenkonten (Shared Accounts) ist unzulässig.

Administrationsrechte sind ausschließlich entsprechend den jeweiligen Aufgaben und Verantwortlichkeiten nach dem Prinzip der minimal erforderlichen Berechtigung (Least Privilege) zu vergeben. Die Berechtigungen müssen rollenbasiert verwaltet sowie jederzeit nachvollziehbar dokumentiert werden.

Sämtliche administrativen Anmeldungen und sicherheitsrelevanten administrativen Aktionen sind zu protokollieren und revisionssicher zu speichern. Die Protokolle müssen eine eindeutige Zuordnung der durchgeführten Tätigkeiten zur jeweils handelnden Person ermöglichen.

Die Einrichtung, Änderung, Sperrung und Löschung administrativer Benutzerkonten hat nach einem dokumentierten Berechtigungs- und Freigabeprozess zu erfolgen.

2.2.3. Service Desk / Hotline

Der Auftragnehmer stellt einen zentralen deutschsprachigen Service Desk als Single Point of Contact (SPOC) für alle Störungen, Service Requests und Betriebsanfragen zur Verfügung. Der Service Desk muss an Werktagen (Montag bis Freitag, ausgenommen gesetzliche Feiertage in Niedersachsen) in der Zeit von **08:00 Uhr bis 18:00 Uhr** telefonisch, per E-Mail erreichbar sein (siehe Kapitel: 6 - Service Level). Der Bearbeitungsstatus aller Vorgänge muss jederzeit nachvollziehbar sein. Eskalationsverfahren sowie Reaktions- und Wiederherstellungszeiten richten sich nach den vereinbarten Service Level Agreements (SLA).

Das Ticketsystem steht dem Auftraggeber 24 x 7 x 365 für die Erfassung zur Verfügung und sollte nach Möglichkeit auch die Einsicht von Störungen, Service Requests und Änderungsanfragen bereitstellen.

Für Störungen der Priorität P1 (kritische Betriebsstörung) stellt der Auftragnehmer eine 24 x 7 x 365 Rufbereitschaft sicher. Kritische Störungen werden unabhängig von den Servicezeiten gemäß den vereinbarten Service Level Agreements bearbeitet.

Der Service Desk muss mindestens folgende Anforderungen erfüllen:

- + Erreichbarkeit an Werktagen von Montag bis Freitag zwischen 08:00 Uhr bis 18:00 Uhr.
- + Bereitstellung einer deutschsprachigen Kommunikation.
- + Annahme von Störungen, Service Requests und Eskalationen.
- + Erfassung sämtlicher Vorgänge in einem Ticket-System.
- + Vergabe einer eindeutigen Ticketnummer.
- + Nachvollziehbare Dokumentation des Bearbeitungsstatus.

- + Bereitstellung einer webbasierten Ticketübersicht für den Auftraggeber.
- + Möglichkeit zur Kontaktaufnahme per E-Mail und Telefon.

2.2.4. Request Fulfillment

Der Auftragnehmer muss ein Verfahren zur Bearbeitung von Service Requests bereitstellen.

Service Requests umfassen insbesondere:

- + Bereitstellung zusätzlicher virtueller Ressourcen.
- + Anpassung von Speicher- und Netzwerkressourcen.
- + Benutzer- und Berechtigungsanforderungen.
- + Bereitstellung von Systeminformationen und Auswertungen.
- + Durchführung standardisierter Betriebsaufgaben.

Der Auftragnehmer muss:

- + Service Requests über das Ticket-System annehmen.
- + Bearbeitungsstatus transparent bereitstellen.
- + Standardleistungen dokumentieren.
- + Bearbeitungszeiten gemäß den vereinbarten Service Levels einhalten.

2.2.5. Kapazitätsmanagement und Monitoring

Der Auftragnehmer überwacht kontinuierlich die Auslastung sämtlicher bereitgestellter Infrastrukturressourcen (Compute, CPU, Arbeitsspeicher, SAN, NAS, Netzwerk sowie Backup-Kapazitäten). Kapazitätsengpässe sind frühzeitig zu erkennen und dem Auftraggeber mit konkreten Handlungsempfehlungen mitzuteilen. Erweiterungen der Ressourcen müssen im laufenden Betrieb ohne Betriebsunterbrechung möglich sein. Regelmäßige Kapazitätsberichte sind bereitzustellen.

Der Leistungsumfang umfasst mindestens:

- + Überwachung der physischen Infrastruktur.
- + Überwachung der Virtualisierungsplattform.
- + Überwachung der bereitgestellten VM
- + Überwachung der Betriebssysteme.
- + Überwachung der Netzwerkkomponenten.
- + Überwachung der Storage-Systeme.
- + Überwachung der Datensicherungsprozesse.

Mindestens folgende Parameter sind zu überwachen:

- + Verfügbarkeit der Systeme.

- + CPU-Auslastung.
 - Alarmierung bei CPU > 85 %
- + Arbeitsspeicherauslastung.
 - Alarmierung bei RAM > 85 %
- + Speicherplatzbelegung.
 - Alarmierung bei Speicherplatz < 15 %
- + Netzwerkverbindungen.
- + Netzwerklatenzen.
- + Storage-Auslastung.
- + Storage-Performance.
- + Systemdienste.
- + Betriebssystemereignisse.
 - Alarmierung bei Ausfall einer VM
- + Backup
 - Alarmierung bei Backup-Fehlern

Bei Erreichen definierter Schwellwerte oder bei Störungen muss automatisch ein Incident erzeugt werden.

Der Auftragnehmer muss kritische Störungen eigenständig analysieren und geeignete Maßnahmen zur Wiederherstellung des Betriebs einleiten.

Monitoringdaten sind mindestens 12 Monate vorzuhalten.

Mindestanforderungen:

- + Rohdaten (z. B. 1-Minuten- oder 5-Minuten-Werte): mindestens 90 Tage
- + Verdichtete Monitoringdaten (Stunden- oder Tageswerte): mindestens 12 Monate
- + SLA- / Verfügbarkeitsdaten, Audit- und Sicherheitsprotokolle: mindestens 24 Monate

2.2.6. Automatisierung von Routineaufgaben

Der Auftragnehmer setzt geeignete Automatisierungsverfahren ein, um wiederkehrende Betriebsaufgaben standardisiert und reproduzierbar auszuführen. Hierzu gehört insbesondere die automatisierte Bereitstellung von Ressourcen, Konfigurationsänderungen, geplante Neustarts, Wartungsaufgaben, Überwachungsprozesse sowie Standard-Reports. Ziel ist die Erhöhung der Betriebssicherheit, Qualität und Nachvollziehbarkeit bei gleichzeitiger Reduzierung manueller Eingriffe.

2.2.7. Incident- und Problemmanagement

Der Auftragnehmer betreibt Incident- und Problemmanagement nach anerkannten Best Practices (z. B. ITIL). Incidents sind entsprechend ihrer Priorität aufzunehmen, zu klassifizieren, zu bearbeiten und innerhalb der vereinbarten Wiederherstellungszeiten zu beheben. Wiederkehrende oder schwerwiegende Störungen sind im Rahmen des Problemmanagements nachhaltig zu analysieren, Ursachen zu identifizieren und geeignete Maßnahmen zur dauerhaften Fehlerbeseitigung einzuleiten. Über kritische Incidents und deren Ursachen sind Root-Cause-Analysen bereitzustellen.

Der Leistungsumfang für Incident Management umfasst mindestens:

- + Annahme, Erfassung, Klassifizierung und Bearbeitung von Störungen über ein Ticket-System
- + Eindeutige Zuordnung einer Priorität je Störung
- + Überwachung der Bearbeitungszeiten gemäß den vereinbarten Service Levels
- + Dokumentation aller Bearbeitungsschritte im Ticket-System
- + Durchführung von Eskalationen bei drohenden oder tatsächlichen SLA-Verletzungen
- + Information des Auftraggebers über größere Störungen und deren Auswirkungen
- + Bereitstellung eines deutschsprachigen Service Desks während der vereinbarten Servicezeiten

Der Auftragnehmer muss monatlich über Anzahl, Art, Bearbeitungsdauer und Status der Störungen berichten.

Der Leistungsumfang für Problem Management umfasst mindestens:

- + Analyse wiederkehrender Incidents
- + Identifikation von Fehlerursachen
- + Erstellung und Pflege von Known Errors
- + Definition und Umsetzung nachhaltiger Korrekturmaßnahmen
- + Dokumentation der Ursachenanalyse und der getroffenen Maßnahmen

Der Auftragnehmer muss den Auftraggeber über identifizierte Probleme mit Auswirkungen auf den Servicebetrieb informieren.

2.2.8. Change Management

Der Auftragnehmer muss ein dokumentiertes Change-Management für Änderungen an der bereitgestellten Infrastruktur betreiben.

Der Prozess muss mindestens folgende Anforderungen erfüllen:

- + Planung, Bewertung, Genehmigung und Dokumentation aller produktionsrelevanten Änderungen.
- + Bewertung technischer und betrieblicher Risiken vor der Umsetzung.
- + Definition von Rückfallverfahren für kritische Änderungen.
- + Information des Auftraggebers vor geplanten Änderungen mit möglicher Auswirkung auf die bereitgestellten Services.
- + Dokumentation erfolgreicher und fehlgeschlagener Änderungen.

Notfalländerungen sind gesondert zu kennzeichnen und nachträglich zu dokumentieren.

2.2.9. Eskalationsverfahren

Für fachliche, technische und organisatorische Eskalationen ist ein abgestuftes Eskalationsverfahren beim Auftragnehmer vorzusehen.

Das Eskalationsverfahren muss mindestens folgende Anforderungen erfüllen:

- + Fachliche Eskalation bei ausbleibender Problemlösung.
- + Management-Eskalation bei drohender oder eingetretener SLA-Verletzung.
- + Benennung fester Ansprechpartner für operative und organisatorische Eskalationen.
- + Dokumentation aller Eskalationen im Ticket-System.
- + Information des Auftraggebers über kritische Störungen und Eskalationen.

Für Störungen der Priorität P1 muss unverzüglich eine Eskalation an den zuständigen Betriebsverantwortlichen des Auftragnehmers erfolgen.

2.2.10. Release- und Patchmanagement

Der Auftragnehmer plant, testet und implementiert sicherheitsrelevante Patches, Hotfixes sowie Hersteller-Releases für die von ihm verantworteten Infrastrukturkomponenten. Änderungen erfolgen gemäß einem abgestimmten Change- und Releaseprozess innerhalb definierter Wartungsfenster. Kritische Sicherheitsupdates sind zeitnah einzuspielen. Vor produktiven Änderungen sind Auswirkungen auf Betrieb und Verfügbarkeit zu bewerten.

Alle Änderungen vor der Umsetzung mit dem Auftraggeber abzustimmen und sind nachvollziehbar zu dokumentieren.

Der Auftragnehmer muss ein geregeltes Patch- und Update-Management für die bereitgestellten Infrastruktur- und Betriebssystemkomponenten betreiben.

Der Leistungsumfang umfasst mindestens:

- + Regelmäßige Prüfung verfügbarer Sicherheitsupdates.
- + Planung, Durchführung und Steuerung von Releases.

- + Bewertung von Risiken und Auswirkungen.
- + Durchführung von Sicherheits- und Stabilitätsprüfungen vor Produktivsetzung.
- + Dokumentation aller Releases und Updates
- + Information des Auftraggebers über geplante Releases.
- + Sicherstellung der Nachvollziehbarkeit aller Änderungen.
- + Information des Auftraggebers über geplante Wartungsmaßnahmen.

Für sicherheitskritische Schwachstellen gelten die Anforderungen gemäß 2.16 - IT-Sicherheit.

Updates dürfen ausschließlich innerhalb der vereinbarten Wartungsfenster durchgeführt werden und den vereinbarten Servicebetrieb nicht beeinträchtigen. Erforderliche Wartungsfenster sind mit dem Auftraggeber abzustimmen.

Der Auftragnehmer muss die erfolgreiche Durchführung dokumentieren und auf Anforderung nachweisen.

Vor der Installation produktiver Updates muss ein Rückfallverfahren definiert sein.

2.2.11. Backup & Restore

Der Auftragnehmer muss ein Verfahren zur Datensicherung und Wiederherstellung bereitstellen.

Die Datensicherung muss mindestens folgende Komponenten umfassen:

- + Virtuelle Server (VM)
- + Datenbanken
- + Betriebssysteme
- + Systemkonfigurationen
- + Dateisysteme
- + Anwendungsdaten.

Mindestens folgende Sicherungen sind durchzuführen:

- + Stündlich inkrementeller Snapshot
- + Tägliche Vollsicherung.

Die Aufbewahrungsfristen müssen mindestens betragen:

- + Snapshots: 1 Wochen
- + Tagesstände: 4 Wochen
- + Wochenstände: 8 Wochen
- + Monatsstände: 6 Monate

Sämtliche Sicherungsdaten sind ausschließlich in Rechenzentren innerhalb Deutschlands zu speichern. Die Sicherungsdaten sind verschlüsselt abzulegen und gegen unberechtigten Zugriff zu schützen. Der Auftragnehmer muss die erfolgreiche Durchführung der Datensicherung überwachen und dokumentieren.

Die Wiederherstellung einzelner Dateien, Systeme oder virtueller Maschinen muss auf Anforderung des Auftraggebers möglich sein.

Der Auftragnehmer hat mindestens einmal jährlich sowie nach wesentlichen Änderungen der Infrastruktur einen Wiederherstellungstest (Disaster-Recovery-Test) durchzuführen und dem Auftraggeber die Ergebnisse einschließlich der erreichten RTO- und RPO-Werte zu dokumentieren.

Der Auftraggeber wird für die Archivierung der Datenbestände ein Backup über die Applikation VEEAM erstellen und ins eigene Rechenzentrum übertragen.

2.3. Leistungsort

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.3 – Leistungsort“ des EVB-IT Cloud Kriterienkatalogs.

Abweichend von Ziffer 4 EVB-IT Cloud-AGB erfolgt die Verarbeitung von Daten des Auftraggebers durch den Auftragnehmer nicht beschränkt auf die EU und den EWR sowie, sofern ein Angemessenheitsbeschluss gem. Art. 45 DSGVO besteht, die Schweiz, sondern **nur innerhalb der Bundesrepublik Deutschland**.

2.4. Georedundanz

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.4 – Georedundanz“ des EVB-IT Cloud Kriterienkatalogs.

Die Cloud-Infrastruktur muss generell und im Punkt Georedundanz die Standard C5-Kriterien und die vereinbarten Verfügbarkeits- und Wiederanlaufanforderungen erfüllen.

Eine darüberhinausgehende Georedundanz gemäß dem **C5-Zusatzkriterium PS-02** mit mehr als zwei georedundanten Standorten ist nicht Bestandteil des Leistungsumfangs.

2.5. Übergabepunkt

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.5 – Übergabepunkt“ des EVB-IT Cloud Kriterienkatalogs.

Abweichend von Ziffer 5.1. der EVB-IT Cloud AGB ergibt sich der Übergabepunkt wie nachfolgend beschrieben:

Der Auftragnehmer stellt die vollständige Kommunikationsverbindung zwischen der Managed Cloud und den Standorten des Auftraggebers bereit.

Dies umfasst insbesondere:

- + Bereitstellung und Betrieb der Firewall-Infrastruktur im Rechenzentrum
- + Bereitstellung und Betrieb der VPN-Gateways
- + Einrichtung und Betrieb der verschlüsselten Site-to-Site-VPN-Verbindungen
- + Routing zwischen den vereinbarten Netzsegmenten
- + Überwachung und Wartung der VPN-Verbindungen
- + Entstörung der vom Auftragnehmer bereitgestellten Kommunikationsinfrastruktur

Der Übergabepunkt befindet sich an den LAN-Schnittstellen der Router bzw. Firewalls an den Standorten des Gesamtauftraggebers.

Ab diesem Übergabepunkt ist der jeweilige Auftraggeber für den Betrieb seines lokalen Netzwerks (LAN), der Endgeräte sowie der lokalen Infrastruktur verantwortlich, sofern diese nicht ausdrücklich Bestandteil des Leistungsumfangs des Auftragnehmers sind.

2.6. Bereitstellungszeitpunkt

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.6 – Bereitstellungszeitpunkt“ des EVB-IT Cloud Kriterienkatalogs.

Die vollständige Betriebsbereitschaft der ausgeschriebenen Leistungen erfolgt basierend auf dem jeweiligen Abruf. Die initiale Bereitstellung ist zum 01.01.2027 geplant. Für die weiteren, angedachten Abrufe vgl. Kapitel 1.2 und Angaben im Preisblatt.

2.7. Nutzer

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.7 – Nutzer“ des EVB-IT Cloud Kriterienkatalogs.

Die angebotene Managed Cloud muss den gleichzeitigen Zugriff der berechtigten Benutzer auf die bereitgestellten Anwendungen und Dienste unterstützen.

Zum Zeitpunkt der Erstinbetriebnahme ist von ca. 60 internen Anwendern auszugehen. Die Managed Cloud Infrastruktur ist darüber hinaus so auszulegen, dass sie ohne grundlegende Änderungen der Architektur auf über 500 zusätzliche externe Projekt- und Bauleitungsmitarbeiter erweitert werden kann.

Die Benutzerverwaltung erfolgt zentral über das Active Directory des jeweiligen Auftraggebers. Die angebotene Lösung muss die Authentifizierung und Autorisierung über den bestehenden Verzeichnisdienst unterstützen.

Die Managed Cloud Infrastruktur darf die Anzahl der verwaltbaren Benutzer grundsätzlich nicht begrenzen.

Soweit für einzelne Anwendungen benannte Benutzer (Named User) oder gleichzeitig aktive Benutzer (Concurrent User) lizenzrechtlich relevant sind, sind diese Einschränkungen gesondert auszuweisen. Der Austausch benannter Benutzer muss jederzeit ohne zusätzliche technische oder organisatorische Einschränkungen möglich sein.

2.8. Nutzerkreis

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.8 – Nutzerkreis“ des EVB-IT Cloud Kriterienkatalogs.

Alle Mitarbeiter des Auftraggeber Dachgesellschaft Bauvorhaben Hochschulmedizin Niedersachsen mbH (DBHN) am Standort „Andreaestraße 7, 30159 Hannover“ und aus dem „Home-Office“ der DBHN-Mitarbeiter.

Alle Mitarbeiter der Firma Baugesellschaft UMG mbH (BauG UMG) am Standort „Robert-Koch-Straße 34, 37075 Göttingen“ und aus dem „Home-Office“ der Mitarbeiter.

Alle Mitarbeiter der Firma Hochschulmedizin Hannover Baugesellschaft mbH (HBG) am Standort „Podbielskistraße 386, 30659 Hannover“ und aus dem „Home-Office“ der Mitarbeiter.

Der Nutzerkreis umfasst auch externe Projektbeteiligte, die auf einzelne Fachanwendungen zugreifen, sofern dies für die Projektbearbeitung erforderlich ist.

Die Benutzer werden entsprechend ihrer Aufgaben und Berechtigungen in unterschiedliche Nutzergruppen eingeteilt. Um den technischen Support für die Fachanwendungen zu gewährleisten ist der Zugriff auf die einzelnen Fachanwendungen und teilweise auf die Konfiguration des VM notwendig. Die Verwaltung der Zugriffsrechte erfolgt rollenbasiert über das Active Directory des Auftraggebers.

Folgende Nutzergruppen werden benötigt:

- + Administratoren
Mitarbeitende des Auftraggebers mit administrativen Berechtigungen für die virtuellen Maschinen, Fachanwendungen und Benutzerverwaltung.
- + Key User/Supportmitarbeiter
Fachliche Ansprechpartner der jeweiligen Fachbereiche mit erweiterten

Berechtigungen innerhalb der Fachanwendungen. Sie unterstützen den First-Level-Support und koordinieren fachliche Fragestellungen.

+ Standardanwender

Mitarbeitende der drei Unternehmen mit Zugriff auf die jeweils freigegebenen Fachanwendungen.

+ Externe Projektbeteiligte

Benutzer aus beauftragten Unternehmen mit projektbezogenem Zugriff auf definierte Anwendungen und Daten.

Der Zugriff erfolgt ausschließlich nach Freigabe durch den Auftraggeber.

2.9. Nutzungsort

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.9 – Nutzungsort“ des EVB-IT Cloud Kriterienkatalogs.

Abweichend von Ziffer 14.1 EVB-IT Cloud-AGB ist das Recht zur Nutzung der Leistung örtlich auf das Gebiet der Vertragsstaaten der EU und des EWR sowie der Schweiz beschränkt.

2.10. Identitäts- und Berechtigungsmanagement (IDM)

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.10 – Identitäts- und Berechtigungs-management“ des EVB-IT Cloud Kriterienkatalogs.

C5 Zusatzkriterium IDM-02:

Der Auftragnehmer bietet dem Auftraggeber einen Self-Service an, mit welchem diese Zugangs- und Zugriffsberechtigungen eigenständig vergeben und ändern können.

Der Auftragnehmer sorgt durch technische Maßnahmen dafür, dass die Nutzer keine Leistungen beauftragen können, welche nicht vom Leistungsumfang des Vertrages umfasst, sind

2.11. Endgeräte

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.12 – Endgeräte“ des EVB-IT Cloud Kriterienkatalogs.

Der Zugriff auf die Managed Cloud Infrastruktur bzw. auf die Fachanwendungen muss mindestens über folgende Endgeräte bzw. Zugriffsarten möglich sein:

- + Windows-basierte Arbeitsplatzrechner und Notebooks,
- + aktuelle Webbrowser ohne Installation zusätzlicher Client-Software, sofern dies durch die jeweilige Fachanwendung unterstützt wird,
- + Terminalserver- bzw. Remote-Desktop-Umgebungen,

- + mobile Endgeräte (Smartphones und Tablets), sofern die jeweilige Fachanwendung hierfür geeignete Zugriffsverfahren bereitstellt.

Die Managed Cloud Infrastruktur ist so auszulegen, dass sie den gleichzeitigen Zugriff interner und externer Anwender unterstützt. Insbesondere ist die Architektur für den späteren Ausbau auf bis zu ca. 500 externe Projekt- und Bauleitungsmitarbeiter auszulegen, ohne dass die vereinbarten Service Levels beeinträchtigt werden.

2.12. Speicher-Größe (für Speicherung von Auftraggeberdaten)

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.13 – Speicher-Größe (für Speicherung von Auftraggeberdaten)“ des EVB-IT Cloud Kriterienkatalogs.

Speicherung beim Auftragnehmer ist dynamisch und umfasst ab dem Bereitstellungszeitpunkt folgenden Speicherumfang:

2.12.1. SAN je VM

- + SAN-Ressourcen
- + Erstinstallation und Erweiterung nach Abruf
- + Erweiterung im laufenden Betrieb ohne Betriebsunterbrechung

2.12.2. NAS

- + NAS-Ressourcen
- + Erstinstallation und Erweiterung nach Abruf
- + Erweiterung im laufenden Betrieb ohne Betriebsunterbrechung

2.13. Art der Anbindung

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.14 – Art der Anbindung“ des EVB-IT Cloud Kriterienkatalogs.

Der Auftragnehmer stellt eine hochverfügbare, redundante und verschlüsselte Standortanbindung bereit. Zulässig sind IPSec-VPN, SD-WAN oder technisch gleichwertige Lösungen. Die Anbindung erfolgt über ein bis zwei voneinander unabhängige Übertragungswege mit einer symmetrischen Bandbreite von jeweils mindestens 1 Gbit/s. Die Bereitstellung, der Betrieb, die Überwachung und die Entstörung der Anbindung sind Bestandteil der Managed Cloud Services.

2.13.1. Anbindung der Managed Cloud

Die Anbindung muss mindestens folgende Anforderungen erfüllen:

- + Bereitstellung einer verschlüsselten Site-to-Site-Verbindung zwischen den Standorten des Auftraggebers und dem Rechenzentrum
- + Einsatz einer sicheren VPN-Technologie (mindestens IPSec nach aktuellem Stand der Technik)
- + Bereitstellung redundanter Kommunikationswege ohne Single Point of Failure
- + Unterstützung einer symmetrischen Datenübertragung
- + Auslegung auf den produktiven Betrieb der bereitgestellten Anwendungen
- + Überwachung der Leitungen durch den Auftragnehmer
- + automatische Wiederherstellung der Verbindung bei Leitungs- oder Hardwareausfall
- + Bereitstellung und Betrieb der erforderlichen Router-, Firewall- und VPN-Komponenten
- + Dokumentation der Netzwerktopologie und der Routingkonfiguration

Die Kommunikationsanbindung muss während der Vertragslaufzeit bedarfsgerecht erweitert werden können.

2.13.2. Remote-Access / VPN-Einwahl

Der Auftragnehmer stellt einen Remote-Access-Service einschließlich VPN-Gateway, Authentifizierung, Autorisierung und sicherer verschlüsselter Kommunikation für berechtigte Benutzer bereit. Der Zugriff muss sowohl von Home-Office-Arbeitsplätzen als auch von mobilen Arbeitsplätzen über öffentliche Internetverbindungen möglich sein. Der Dienst muss hochverfügbar ausgelegt sein und eine Mehrfaktor-Authentifizierung unterstützen.

2.14. Bandbreite der Anbindung des Auftragnehmers

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.15 – Bandbreite der Anbindung des Auftragnehmers an das Internet, die für den Auftraggeber zur Verfügung steht“ des EVB-IT Cloud Kriterienkatalogs.

Die Anbindung erfolgt über eine, später über mindestens **zwei** voneinander unabhängige Übertragungswege mit einer symmetrischen Bandbreite von jeweils mindestens 1 Gbit/s.

Jeder Unternehmensstandort wird mit der beschriebenen Anbindung angeschlossen.

2.15. Datensicherung*

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.16 – Datensicherung“ des EVB-IT Cloud Kriterienkatalogs.

Ergänzend zu Ziffer 7 EVB-IT Cloud-AGB gilt Folgendes:

Der Auftragnehmer ist zur Planung, Durchführung, Überwachung und Dokumentation der Datensicherung sämtlicher durch ihn bereitgestellten Infrastruktur- und Speicherkomponenten verpflichtet.

Die Datensicherung umfasst mindestens:

- + virtuelle Maschinen
- + Betriebssysteme
- + Datenbanken
- + SAN-Verzeichnisse
- + NAS-Dateifreigaben
- + Konfigurationsdaten der Infrastruktur
- + Firewall- und Netzwerkkonfigurationen (soweit für den Wiederanlauf erforderlich)

2.15.1. Backup-Verfahren

Die Datensicherung muss mindestens folgende Backup-Verfahren unterstützen:

- | | |
|---------------------------|---|
| + Image-Backup | Vollständige Sicherung der virtuellen Maschinen einschließlich Betriebssystem und Konfiguration |
| + Dateibasierte Sicherung | Sicherung der NAS-Dateifreigaben |
| + Datenbanksicherung | Konsistente Sicherung der SQL-Datenbanken einschließlich Transaktionsprotokolle |
| + Konfigurationssicherung | Sicherung der Infrastrukturkonfiguration. |

2.15.2. Backup-Intervall

Die Datensicherung muss in folgenden Backup-Intervallen durchgeführt werden.

- | | |
|------------------------------|---------------------|
| + Virtuelle Maschinen | täglich |
| + Datenbanken | täglich Vollbackup |
| + SQL-Transaktionsprotokolle | alle 15 Minuten |
| + SAN, NAS | täglich |
| + Konfigurationen | nach jeder Änderung |

2.15.3. Aufbewahrungsfristen

- | | |
|---------------|-----------|
| + Täglich | 30 Tage |
| + wöchentlich | 12 Wochen |
| + monatlich | 12 Monate |

- + jährlich
 - + Konfigurationen
- optionale Abstimmung
nach jeder Änderung

2.15.4. Backup-Speicherort

Der Auftragnehmer speichert die Datensicherungen

- + innerhalb Deutschlands
- + in einem vom Produktivsystem getrennten Speicherbereich
- + verschlüsselt
- + redundant

Mindestens eine Sicherungskopie ist in einem zweiten Brandabschnitt oder einem zweiten Rechenzentrum innerhalb Deutschlands aufzubewahren.

2.15.5. Restore

Der Auftragnehmer muss mindestens folgende Wiederherstellungen unterstützen.

- + komplette VM
- + einzelne VM-Dateien
- + komplette SQL-Datenbank
- + einzelne Datenbank
- + einzelne Dateien aus NAS
- + komplette NAS-Freigabe
- + vollständiger Server

2.15.6. Wiederherstellungstests

Der Auftragnehmer führt regelmäßig Wiederherstellungstests durch.

Mindestens:

- + jährlich vollständiger Disaster-Recovery-Test
- + halbjährlicher Restore-Test einer virtuellen Maschine
- + monatlicher Test einzelner Datei-Wiederherstellungen

Die Ergebnisse sind dem Auftraggeber im Service Review Meeting vorzulegen.

2.15.7. Verschlüsselung

Alle Backups müssen

- + verschlüsselt gespeichert werden

- + verschlüsselt übertragen werden
- + gegen unberechtigten Zugriff geschützt werden

Zusätzlich zum C5 Basiskriterium OPS-08 ist der Auftragnehmer verpflichtet, den Auftraggeber auf dessen Anforderung über die Ergebnisse der durchgeführten Wiederherstellungstests zu informieren. Wiederherstellungstests sind in das Notfallmanagement des Auftragnehmers eingebettet.

Der Auftraggeber ist für folgende Datensicherungen selbst verantwortlich, wobei der Auftragnehmer die dazu erforderlichen Funktionalitäten zur Verfügung stellt:

- + Datenbank Backup in Verantwortung des Auftraggebers: SQL-Server Backup über VEEAM-Backup-Server zum Standort des Auftraggebers

Der Auftragnehmer erläutert zu Leistungsbeginn unaufgefordert sein **Backup- und Restore-Konzept** basierend auf den Vorgaben mit nachfolgenden Mindestangaben

- + Sicherungsstrategie (Voll-, inkrementelle und ggf. differenzielle Sicherungen)
- + Aufbewahrungsfristen
- + Speicherorte
- + Verschlüsselung
- + Wiederherstellungsverfahren
- + Wiederherstellungstests
- + Verantwortlichkeiten
- + RPO- und RTO-Vorgaben.

2.16. IT-Sicherheit

Die nachfolgenden Anforderungen orientieren sich am Punkt „1.18 – IT-Sicherheit“ des EVB-IT Cloud Kriterienkatalogs.

Abweichend von Ziffer 1.2 EVB-IT Cloud-AGB ist nicht nur die Einhaltung der C5 Basiskriterien, sondern auch der folgenden C5 Zusatzkriterien geschuldet

- + OPS-22: Sicherheitspatches werden ab dem Zeitpunkt ihrer Verfügbarkeit* in Abhängigkeit des nach der jüngsten Version des Common Vulnerability Scoring Systems (CVSS) eingeordneten Schweregrades der dadurch adressierten Schwachstellen eingespielt:

Kritisch	(CVSS = 9.0 - 10.0):	3 Stunden
Hoch	(CVSS = 7.0 - 8.9):	3 Tage
Mittel	(CVSS = 4.0 - 6.9):	1 Monat

Niedrig (CVSS = 0.1 - 3.9): 3 Monate

Abweichend bzw. ergänzend zu Ziffer 6.2 EVB-IT Cloud-AGB wird vereinbart, dass

- + das vom Auftragnehmer implementierte Sicherheitskonzept und sein ISMS auf ISO 27001 und BSI IT-Grundschutz in der jeweils geltenden Fassung basiert.
- + das Notfall-Management gemäß BSI-Standard 100-4 bzw. nach dessen Inkrafttreten BSI Standard 200-4 und ISO 22301 (Business Continuity Management - BCM) erfolgt.
- + der Auftragnehmer die Umsetzung der Vorgaben zur IT-Sicherheit durch BSI C5 Typ 2 (C5 Testat) nachweisen muss.

2.17. Verfügbarkeit

Die nachfolgenden Anforderungen orientieren sich am Punkt „**2 – Verfügbarkeit**“ des EVB-IT Cloud Kriterienkatalogs.

Abweichend zu Ziffer 8 EVB-IT Cloud-AGB

- + schuldet der Auftragnehmer während der Betriebszeit* eine Verfügbarkeit* von mindestens der Verfügbarkeitsklasse* **2 des BSI (99,9%)** im Bezugszeitraum,
- + ist die Betriebszeit* die Zeit von Montag bis Freitag **von 06:00 bis 22:00 Uhr**.
- + besteht in der Zeit **von 08:00 bis 18:00 Uhr** von Montag bis Freitag eine Kernbetriebszeit*. Zusätzlich wird teilweise am Wochenende (Samstag-Sonntag, sowie an Feiertagen) zur gleichen Zeit gearbeitet.
- + ist die Zeit **von 22:00 bis 06:00 Uhr** an Wochentagen (Montag-Freitag) sowie an Samstagen, Sonntagen und Feiertagen die Zeit geplanter Nichtverfügbarkeit (z.B. für Wartungsarbeiten) und wird bei der Berechnung der Verfügbarkeit* nicht berücksichtigt.

2.18. Gutschriften bei Nichtverfügbarkeit

Die nachfolgenden Anforderungen orientieren sich am Punkt „**2.1 – Gutschriften bei Nichtverfügbarkeit**“ des EVB-IT Cloud Kriterienkatalogs.

Für den Fall der Nichteinhaltung der vereinbarten Verfügbarkeit* die folgende Gutschrift zugunsten des Auftraggebers vereinbart:

Unterschreitung in Prozentpunkten [■]		Gutschrift in Prozent der für den vereinbarten Bezugszeitraum geschuldeten Vergütung in % der betroffenen Betriebspauschale ■ Betroffene Betriebspauschale: Preis-Pos-Nr. Cloud_Betrieb_P15 zzgl. der betroffenen Infrastrukturkomponente P16-P17
> 0	< 1	1%
> = 1	< 2	2%
> = 2	< 3	3%
> = 3	< 4	4%
> = 4		5%

2.19. Reaktions- und Wiederherstellungszeiten

Die nachfolgenden Anforderungen orientieren sich am Punkt „2.2 – Reaktions- und Wiederherstellungszeiten“ des EVB-IT Cloud Kriterienkatalogs.

Die Reaktions- und Wiederherstellungszeiten* sind im Kapitel „6.3- „Service Level Management““ beschrieben.

2.20. Protokollierung

Die nachfolgenden Anforderungen orientieren sich am Punkt „2.3 – Protokollierung“ des EVB-IT Cloud Kriterienkatalogs.

Der Auftragnehmer führt folgende Protokolle:

- + Protokolle über den Sicherheitsstatus des Cloud-Managementsystems (Vollständigkeit, Verfügbarkeit*, Integrität und Vertraulichkeit der verarbeiteten Daten).
- + Protokolle über Art und Zeitpunkte der durchgeführten Datensicherungsmaßnahmen und Rücksicherungen.
- + Die Protokolle sind mindestens sechs Monate revisionssicher aufzubewahren.

2.21. Aktualisierung

Die nachfolgenden Anforderungen orientieren sich am Punkt „2.4 – Aktualisierung“ des EVB-IT Cloud Kriterienkatalogs.

Die Leistungen sind mit jeweils allgemein verfügbaren und vom Hersteller regulär supporteten Programmständen* zu erbringen. Der Auftragnehmer ist zu deren Bereitstellung verpflichtet.

Der Auftragnehmer ist verpflichtet, folgende Programmstände* zu installieren und zu integrieren, sobald verfügbar:

- + Updates*
- + Upgrades*
- + neue Releases/Versionen*
- + neue Firmwarestände

Der Auftragnehmer ist verpflichtet, Programmstände* zur Umsetzung von Änderungen solcher Rechtsvorschriften und technischer Normen gemäß Kapitel „2.2.10 - Release- und Patchmanagement“ zu installieren und zu integrieren. Der Auftragnehmer stellt die geschuldeten Programmstände* innerhalb angemessener Zeit vor, spätestens aber mit dem Inkrafttreten der jeweiligen Vorschrift oder Norm bzw. dem Zeitpunkt der vorgesehenen Änderung bzw. Anpassung. Erfolgt dies nicht spätestens zu diesen Terminen, ist der Auftragnehmer unbeschadet davon verpflichtet, dem Auftraggeber eine Übergangslösung bereitzustellen. Soweit ihm beides zu diesen Terminen zeitlich nicht zumutbar ist, haben sie innerhalb einer angemessenen Frist zu erfolgen.

2.22. Reporting

Die nachfolgenden Anforderungen orientieren sich am Punkt „2.5 – Reporting“ des EVB-IT Cloud Kriterienkatalogs.

Ergänzend zu Ziffer 9 EVB-IT Cloud-AGB hat das Reporting folgende Inhalte:

- + die durchgeführten Einspielungen neuer Programmstände* (z.B. Sicherheitspatches)
- + sämtliche für die Leistungen relevante Sicherheitsvorfälle (Zeitpunkt, Art, und Umfang des Vorfalls) und die vom Auftragnehmer getroffenen Maßnahmen zu deren Beseitigung
- + die durchgeführten Backups und Datenexporte sowie ihre erfolgreiche Verifikation.

Zusätzlich zu Ziffer 9 EVB-IT Cloud-AGB ist für den Auftraggeber während der Nutzung der Leistung in Echtzeit einsehbar, wie viele Managed Cloud Ressourcen (Virtueller Speicher, Virtuelles Netzwerk, Virtuelle CPU-Last, Virtuelles Storage) aktuell in Gebrauch sind (d.h. eine Darstellung der Auslastung der aktuell sich in Gebrauch befindlichen Managed Cloud Ressourcen).

2.23. Mitwirkungsleistungen des Auftraggebers

Die nachfolgenden Anforderungen orientieren sich am Punkt „2.6 – Mitwirkungsleistungen des Auftraggebers“ des EVB-IT Cloud Kriterienkatalogs.

Der Auftraggeber stellt wie der Auftragnehmer einen zentralen Ansprechpartner zur Verfügung (vergl. Kapitel. 2.2.1 - Ansprechpartner / Mitwirkungspflichten).

3. Bestandteile der Managed Cloud: Architektur und Infrastruktur

Die nachfolgenden Anforderungen orientieren sich am Punkt „3 – Sonderkriterien für IaaS und PaaS“ des EVB-IT Cloud Kriterienkatalogs.

Folgende Bestandteile werden für die Managed Cloud beschafft (siehe Preisblatt).

3.1. Virtuelle Maschinen – Inbetriebnahme

siehe Preisblatt - Preis-Pos-Nr.: Cloud_Basis_P1

geplanter Abruf nach aktuellem Stand:

- + 5 Virtuelle Maschinen (16 GB RAM je Core)
- + 68 Cores
- + 1.088 GB RAM
- + SAN-Storage (ca. 19 TB)
- + Einsatz: VM für AD, Applikation- und Datenbankserver im Test- und Produktivbetrieb

siehe Preisblatt - Preis-Pos-Nr.: Cloud_Basis_P2

- + geplanter Abruf nach aktuellem Stand:
- + 6-10 Virtuelle Maschinen (8 GB RAM je Core)
- + 20 Cores
- + 160 GB RAM
- + SAN-Storage (ca. 5 TB)
- + Einsatz: VM für Applikation- und Datenbankserver im Test- und Produktivbetrieb

Alle VMs müssen folgende Grundkonfigurationen einhalten

- + Betriebssystem: 64-Bit Operating System
- + x64-based Processor (Intel/AMD)
- + ≥ 3.0 GHz
- + 10Gbit Ethernet

Natives Host-Betriebssystem

Der Auftragnehmer stellt eine Enterprise-Virtualisierungsplattform bereit, um Virtuelle Maschinen mit Windows Betriebssystem und Windows Anwendungen zu betreiben.

Host-Betriebssystem

- + Vom Hersteller unterstütztes Serverbetriebssystem bzw. Hypervisor als Hostplattform

Virtualisierung

- + Enterprise-Virtualisierungsplattform, zentralem Management und SAN-Integration
- + Installation als Host-Betriebssystem (Parent Partition)
- + vollständige Lizenzierung durch den Auftragnehmer
- + Integration in das Monitoring und Patchmanagement
- + Betrieb entsprechend den Herstellerempfehlungen
- + regelmäßige Sicherheitsupdates
- + Härtung nach Best Practices
- + ausschließliche Nutzung als Virtualisierungshost

3.2. Storage

siehe Preisblatt - Preis-Pos-Nr.: Cloud_Storage_P3 – P4

Die SAN-Anbindung ist vollständig redundant auszuführen. Die VMs sind über mindestens zwei voneinander unabhängige Datenpfade an das Storage-System anzubinden. Die Anbindung muss Multipathing unterstützen und darf keinen Single Point of Failure aufweisen.

3.2.1. SAN

siehe Preisblatt - Preis-Pos-Nr.: Cloud_Storage_P3

SAN-Anbindung

Jede VM muss über mindestens vier (4) Controller erreichbar sein.

Die Festplatten sollen als Thick Eager Zeroed angelegt werden

Wenn die Anzahl der Controller auf 4 begrenzt ist, sollen die Controller für die Datenbankserver folgendermaßen aufgeteilt werden:

Festplatte	Controller
1. Betriebssystem und Software	1
2. SQL Server Datenbankdateien	2
3. SQL Server Protokolldateien	3
4. SQL Server TempDB-Datendateien	4
5. SQL Server Analysis Services Datenbanken	3
6. Projektarbeitsverzeichnis, Datenaustausch- und Importverzeichnis	1

Funktionalen Anforderungen

- + Multipathing getrennte virtuelle Datenträger für Daten, Logs und TempDB
- + optimierte I/O-Verteilung
- + redundante SAN-Anbindung
- + garantierte Performance (IOPS, Bandbreite und Latenz)
- + Leistung in Total IOPS: 25.000
- + Datenrate in MB/s mind.: 1.000
- + Latenz in ms maximal: ≤ 2 ms

SAN-Skalierung

Das SAN-System muss während der Vertragslaufzeit flexibel erweitert werden können.

Der Auftragnehmer gewährleistet:

- + Erweiterung der Speicherkapazität ohne Neuinstallation
- + Erweiterung ohne Unterbrechung des laufenden Betriebs
- + Migration der Daten ohne Datenverlust
- + Überwachung der Speicherauslastung sowie rechtzeitige Information des Auftraggebers bei Erreichen definierter Kapazitätsgrenzen

3.2.2. NAS

siehe Preisblatt - Preis-Pos-Nr.: Cloud_Storage_P4

Der Auftragnehmer stellt ein NAS-System mit folgenden Mindestanforderungen bereit:

- + Erweiterung der Speicherkapazität im laufenden Betrieb (Scale-Up) ohne Betriebsunterbrechung
- + Unterstützung aktueller Dateiprotokolle (SMB 3.x und/oder NFS)
- + Integration in das Identity-Management (z. B. Active Directory)
- + Unterstützung granularer Zugriffsberechtigungen auf Freigaben und Verzeichnisse
- + Snapshot- und Backup-Unterstützung
- + Monitoring der Speicherkapazität und Systemverfügbarkeit
- + redundante Auslegung ohne Single Point of Failure

Der Auftragnehmer stellt bei Bedarf Dateifreigaben für berechtigte externe Benutzer bereit. Der Zugriff erfolgt ausschließlich authentifiziert, verschlüsselt und unter Einhaltung der vom Auftraggeber vorgegebenen Sicherheitsrichtlinien.

Abnahme und Erweiterung des NAS

Das NAS-System muss während der Vertragslaufzeit flexibel erweitert werden können.

Der Auftragnehmer gewährleistet:

- + Erweiterung der Speicherkapazität ohne Neuinstallation
- + Erweiterung ohne Unterbrechung des laufenden Betriebs
- + Migration der Daten ohne Datenverlust
- + Überwachung der Speicherauslastung sowie rechtzeitige Information des Auftraggebers bei Erreichen definierter Kapazitätsgrenzen

3.3. RAM-Speichererweiterung

RAM-Speichererweiterung „Cloud_RAM_P5“ mit Inbetriebnahme bei Bedarf, um die verschiedene VM zu erweitern.

3.4. Kommunikationssicherheit

COS-06 C5 Zusatzkriterium: Die sichere Trennung durch physisch getrennte Netze oder durch stark verschlüsselte VLANs ist sichergestellt. Zur Definition einer starken Verschlüsselung ist die Technische Richtlinie TR-02102 des BSI zu berücksichtigen.

4. Erweiterung und Reduzierung der Leistung

Die nachfolgenden Anforderungen orientieren sich am Punkt „4 – Erweiterung und Reduzierung der Leistung“ des EVB-IT Cloud Kriterienkatalogs.

Alle Systeme sind innerhalb von 4 Wochen nach Anforderung durch den Auftraggeber betriebsbereit bereitzustellen.

5. Dienstleistungen

5.1. Überblick

Der Auftragnehmer ist für die Einrichtung, den Betrieb und die Betreuung der Managed Cloud Infrastruktur verantwortlich. Er kümmert sich um alle anfallenden Themen bis zur Betriebssystemebene und unterstützt den Auftraggeber hinsichtlich verschiedener Fragestellungen zu den Virtuellen Maschinen und zur Unterstützung der Applikation- und Datenmigration.

Der Auftraggeber und von ihm zusätzlich betraute Dienstleister kümmern sich vorrangig um die betriebenen Virtuellen Maschinen und die installierten Fachanwendungen/Applikationen.

5.2. Einmalige Projekt-/Bereitstellungskosten

Einrichtung der Managed-Cloud-Umgebung (Preis-Pos-Nr.: **Cloud_Bereit_P06**)

Bereitstellung und Einrichtung einer souveränen Managed Cloud einschließlich der vollständigen Infrastruktur im Rechenzentrum. Die Leistung umfasst die Einrichtung der Compute-, Storage-, Netzwerk- und Sicherheitskomponenten sowie die betriebsbereite Bereitstellung der Managed Cloud Umgebung entsprechend den Anforderungen des Auftraggebers.

Installation und Grundkonfiguration der Hypervisor-Lösung (Preis-Pos-Nr.: **Cloud_Bereit_P07**)

Installation, Härtung und Grundkonfiguration der Virtualisierungs-Lösung einschließlich Installation des Host-Betriebssystems bzw. der Hypervisor-Schicht, Integration in die Managementplattform, Einrichtung der Netzwerkkonfiguration sowie Durchführung aller erforderlichen Funktionstests.

Bereitstellung und Konfiguration des SAN-Systems (Preis-Pos-Nr.: **Cloud_Bereit_P08**)

Bereitstellung, Installation und Konfiguration des Storage Area Networks (SAN) einschließlich Einrichtung der Storage-Switches, Storage-Controller, Storage-Pools, LUNs, Redundanzmechanismen, Performanceparameter und Anbindung an die Virtualisierungsplattform.

Bereitstellung und Konfiguration des NAS-Systems (Preis-Pos-Nr.: **Cloud_Bereit_P09**)

Bereitstellung eines Network Attached Storage (NAS) einschließlich Einrichtung der Dateifreigaben, Speicherbereiche, Berechtigungskonzepte, Active-Directory-Integration, Zugriffsprotokolle sowie Grundkonfiguration für den produktiven Betrieb.

Einrichtung der Monitoring-Plattform (Preis-Pos-Nr.: **Cloud_Bereit_P10**)

Einrichtung und Konfiguration der Monitoring-Lösung zur Überwachung der Infrastrukturkomponenten. Dies umfasst insbesondere Server, Virtualisierung, SAN, NAS, Netzwerk, Firewall, VPN sowie die Konfiguration von Alarmierungen, Schwellwerten und Benachrichtigungen.

Einrichtung der Backup-Infrastruktur (Preis-Pos-Nr.: **Cloud_Bereit_P11**)

Einrichtung der Backup- und Restore-Infrastruktur einschließlich Konfiguration der Backup-Jobs, Sicherungsmedien, Backup-Ziele, Aufbewahrungsrichtlinien, Verschlüsselung, Wiederherstellungstests sowie Dokumentation des Backup-Konzeptes.

Bereitstellung und Grundkonfiguration einer virtuellen Maschine (Preis-Pos-Nr.: **Cloud_Bereit_P12**)

Bereitstellung einer virtuellen Maschine einschließlich Erstellung der VM, Zuweisung der vereinbarten Compute- und Storage-Ressourcen, Installation des Betriebssystems, Netzwerkanbindung, Einbindung in Monitoring und Backup sowie Durchführung eines Funktionstests.

Nach dem initialen Einrichten des Managed Cloud Environment werden in der Phase 2 (vgl. Kapitel 1.2) mindestens drei VM benötigt:

-  AD Domain Controller
-  BI/CPM Applikationsserver
-  BI/CPM Datenbankserver

Die weiteren virtuellen Maschinen sind gemäß aktueller Planung in den folgenden Phasen angedacht.

Einrichtung der VPN-Anbindung (Preis-Pos-Nr.: **Cloud_Bereit_P13**)

Einrichtung einer verschlüsselten Site-to-Site-VPN-Verbindung zwischen dem Rechenzentrum und den Standorten des Auftraggebers für alle Gesellschaften einschließlich Konfiguration der VPN-Gateways, Routing, Firewall-Regeln, Authentifizierung, Redundanzmechanismen und Durchführung der Verbindungstests.

Dokumentation und Betriebsübergabe (Preis-Pos-Nr.: **Cloud_Bereit_P14**)

Erstellung und Übergabe der vollständigen Betriebsdokumentation einschließlich Infrastrukturübersicht, Netzwerkdokumentation, IP-Adressierung, Firewall- und VPN-Konfiguration, Backup- und Restore-Konzept, Betriebs- und Administrationshandbuch sowie Durchführung einer gemeinsamen Betriebsübergabe mit Abnahme der bereitgestellten Leistungen.

5.3. Monatliche Betriebspauschalen

Betrieb und ITSM der Managed-Cloud-Infrastruktur (Preis-Pos-Nr.: **Cloud_Betrieb_P15**)

Betrieb, Überwachung, Administration und Wartung der gesamten Managed Cloud einschließlich Netzwerk-, Firewall-, VPN-, Monitoring-, Backup- und Managementkomponenten. Die Leistung umfasst Incident-, Problem-, Change-, Release-, Patch-, Capacity- und Availability-Management gemäß den vereinbarten Service Levels sowie die kontinuierliche Sicherstellung eines sicheren und hochverfügbaren Betriebs.

Betrieb und ITSM verschiedenen VM (Preis-Pos-Nr.: **Cloud_Betrieb_P16**)

Betrieb, Überwachung und Administration der VM einschließlich Host-Betriebssystem bzw. Hypervisor-Schicht, Ressourcenmanagement, Patchmanagement, Sicherheitsupdates, Monitoring, Backup- und Managementkomponenten, Fehleranalyse und Störungsbeseitigung.

Betrieb und ITSM des Storage (Preis-Pos-Nr.: **Cloud_Betrieb_P17**)

Betrieb, Überwachung und Administration des SAN-Storage einschließlich Storage-Controller, Storage-Pools, Fibre-Channel-Anbindungen, Multipathing, Performanceüberwachung,

Kapazitätsmanagement, Backup- und Managementkomponenten, Firmware- und Sicherheitsupdates, Fehleranalyse sowie Störungsbeseitigung.

Betrieb, Überwachung und Administration des NAS-Systems einschließlich Dateifreigaben, Berechtigungsverwaltung auf Infrastrukturebene, Kapazitätsmanagement, Performanceüberwachung, Firmware- und Sicherheitsupdates, Backup- und Managementkomponenten, Snapshot-Management, Fehleranalyse sowie Störungsbeseitigung.

Die Details zu den Leistungen verbunden mit den monatlichen Betriebspauschalen **Cloud_Betrieb_P15 bis Cloud_Betrieb_P17** sind den Beschreibungen in Kapitel 2.2 zu entnehmen.

5.4. Technische Beratung und Unterstützungsleitung auf Tagespauschalpreisbasis

Technical Consultant (Preis-Pos-Nr.: **Cloud_Betrieb_P18**)

Erbringung technischer Beratungs-, Analyse-, Planungs- und Unterstützungsleistungen, die nicht Bestandteil der vereinbarten Managed Cloud Services sind.

Der Auftragnehmer unterstützt den Auftraggeber bei der Weiterentwicklung der Managed Cloud Infrastruktur sowie bei betrieblichen und technischen Fragestellungen. Hierzu gehören Empfehlungen zur Optimierung von Performance, Sicherheit, Verfügbarkeit, Skalierung, Backup- und Recovery-Konzepten sowie Lizenzierung. Darüber hinaus unterstützt der Auftragnehmer bei der Planung von Erweiterungen, Migrationen und Architekturänderungen und informiert proaktiv über technologische Entwicklungen oder Risiken, die den Betrieb der Managed Cloud beeinflussen können.

6. Service Level

6.1. Verfügbarkeiten

Der Auftragnehmer muss die Einhaltung der vereinbarten Service Levels sicherstellen und nachweisen.

Für die bereitgestellte Infrastruktur gelten mindestens folgende Anforderungen:

- + Verfügbarkeit der bereitgestellten Infrastruktur: mindestens VK2, 99,9 %
- + Geplante Wartungsfenster sind von der Verfügbarkeitsberechnung auszunehmen.
- + Wartungsarbeiten sind mindestens fünf Arbeitstage vor Durchführung anzukündigen.

- + Wartungsarbeiten dürfen den Geschäftsbetrieb des Auftraggebers nur in geringem Umfang beeinträchtigen.

Der Auftragnehmer muss die Einhaltung der Service Levels kontinuierlich überwachen.

6.2. Priorisierung, Reaktions- und Wiederherstellungszeiten

Alle Tickets sind nach ihrer Auswirkung auf den Geschäftsbetrieb zu klassifizieren.

Priorität	Beschreibung	Reaktionszeit * ¹ (Response Time)	Wieder- herstellungszeit * ² in Stunden
P1	Priorität P1 Critical (Systemausfall bzw. Gesamtausfall eines Produktivsystems) Schwerwiegende Störung*	30 Minuten	4
P2	Priorität P2 High (Wesentliche Funktion eingeschränkt) Erhebliche Störung*	2 Stunden	8
P3	Priorität P3 Medium (Teilfunktion gestört) Leichte Störung*	4 Stunden	Nächster Werktag
P4	Priorität P4 Low (Allgemeine Anfrage)	8 Stunden	48

*¹ Reaktionszeit/Bearbeitungszeit/Response Time: Die Reaktionszeit beschreibt den Zeitraum zwischen dem Eingang einer Störungs- oder Serviceanfrage und der ersten qualifizierten Bearbeitung durch den Auftragnehmer. Innerhalb dieser Zeit erfolgten die Annahme, Priorisierung, Analyse und Einleitung der weiteren Bearbeitung des Vorgangs.

Die Reaktionszeit endet mit:

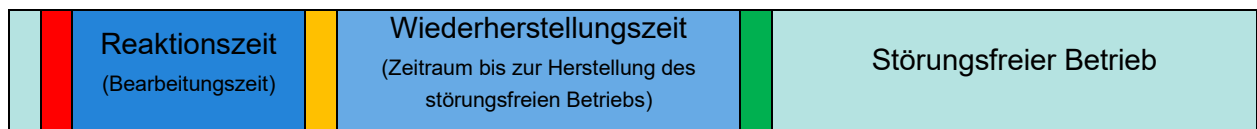
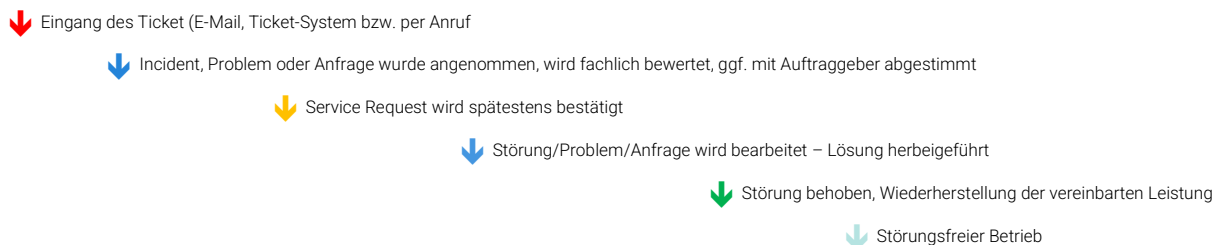
- + Annahme des Tickets
- + Klassifizierung/Priorisierung

- + Beginn der Bearbeitung
- + Kontaktaufnahme zum Kunden (falls erforderlich)

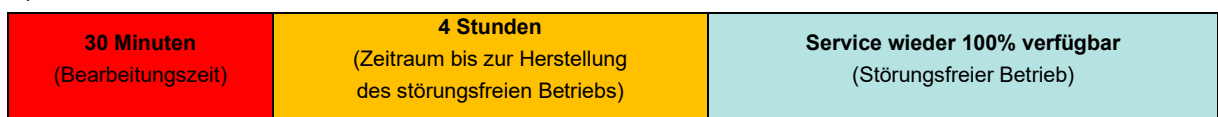
Nicht Bestandteil der Reaktionszeit:

- + Behebung der Störung
- + Wiederherstellung des Services
- + endgültige Lösung

*2 Wiederherstellungszeit/Lösungszeit: Die Wiederherstellungszeit beschreibt den Zeitraum nach der Beendigung der Reaktionszeit und der Wiederherstellung der vereinbarten Servicefunktionalität. Die vollständige Ursachenbeseitigung ist hierfür nicht zwingend erforderlich.



Beispiel für Priorität P1



Der Auftragnehmer hat geeignete Maßnahmen einzuleiten, um die schnellstmögliche Wiederherstellung des Betriebs sicherzustellen.

6.3. Service Level Management

Der Auftragnehmer muss die Einhaltung aller vereinbarten Service Levels überwachen und nachweisen.

Hierzu gehören mindestens:

- + Überwachung der vereinbarten Verfügbarkeit.
- + Überwachung der Reaktions- und Wiederherstellungszeiten.
- + Überwachung der Betriebs- und Servicezeiten.

- + Regelmäßige Berichterstattung an den Auftraggeber.

Der Auftragnehmer muss monatlich einen Servicebericht bereitstellen.

Der Servicebericht muss mindestens folgende Inhalte umfassen:

- + Erreichte Serviceverfügbarkeit.
- + Anzahl und Klassifizierung von Incidents.
- + SLA-Verletzungen.
- + Durchgeführte Changes.
- + Kapazitäts- und Performanceinformationen.
- + Geplante Wartungsmaßnahmen.

6.4. Gutschrift

Bei nichterreichen der geforderten Service Levels wird eine Gutschrift gemäß Kapitel „2.18 - Gutschriften bei Nichtverfügbarkeit“ fällig.

7. Dokumentation

Der Auftragnehmer hat sämtliche für die Bereitstellung, den Betrieb, die Administration und die Weiterentwicklung der Managed Cloud erforderlichen Dokumentationen vollständig, aktuell und in deutscher Sprache bereitzustellen.

Der Auftragnehmer hat sämtliche Änderungen an der produktiven Managed Cloud Infrastruktur im Rahmen des Change-Managements zu dokumentieren. Die Dokumentation ist spätestens fünf Arbeitstage nach erfolgreicher Umsetzung des Changes zu aktualisieren.

Mindestens folgende Dokumentationen sind bereitzustellen:

Projekt- und Betriebsdokumentation

- + Betriebsübergabedokumentation
- + Betriebshandbuch
- + Administrationshandbuch
- + Servicehandbuch einschließlich Service- und Eskalationsprozessen

Architektur- und Systemdokumentation

- + Gesamtübersicht der Managed Cloud Architektur
- + Infrastrukturdiagramme
- + Netzwerk- und Kommunikationspläne
- + Virtualisierungs- und Storage-Konzept

- + VPN- und Firewall-Konfiguration

Sicherheitsdokumentation

- + Rollen- und Berechtigungskonzept
- + Administrationskonzept
- + Multifaktor-Authentifizierung (MFA)
- + Protokollierungs- und Auditkonzept

Betriebsdokumentation

- + Monitoring-Konzept
- + Backup- und Restore-Konzept
- + Archivierungskonzept
- + Patch- und Updatekonzept
- + Notfallvorsorge- und Disaster-Recovery-Konzept einschließlich der RTO- und RPO-Werte

Test- und Abnahmedokumentation

- + Installations- und Inbetriebnahmeprotokolle
- + Funktions- und Integrationstests
- + Backup- und Wiederherstellungstests
- + Hochverfügbarkeits- und Failover-Tests
- + Abnahmeprotokolle

Sämtliche Dokumentationen sind dem Auftraggeber in einem elektronischen Format (z. B. PDF) zu übergeben.

Der Auftragnehmer hat sicherzustellen, dass die Dokumentation jederzeit den aktuellen Stand der bereitgestellten Managed Cloud Umgebung widerspiegelt und auf Anforderung des Auftraggebers unverzüglich aktualisiert zur Verfügung gestellt werden kann.