



VERGABEUNTERLAGEN

20261019

Netzwerkbetrieb Managed Service

Offenes Verfahren (EU) (VgV)

Ausschreibung (Korrektur 6)

AUFTRAGGEBER

Universitätsklinikum Frankfurt

Theodor-Stern-Kai 7, 60590 Frankfurt am Main, Deutschland

12.08.2026

Inhaltsverzeichnis

Vergabeunterlagen	1
Projektinformation	1
Vergabeunterlagen/Dateien	4
Anlage-Bewerbungsbedingungen EU.pdf	4
Anlage-D Datenschutzerklärung.pdf	6
Anlage-A Angebotsschreiben ohne Lose.pdf	9
Bietergemeinschaft und Nachunternehmen	12
Anlage-EN1 Eigenerklärung Nachunternehmen.pdf	12
Anlage-EN2 Verpflichtungserklärung Nachunternehmen.pdf	13
Anlage-EBG Erklärung Bietergemeinschaft.pdf	14
Anlage-BMWK Eigenerklärung Bezug Russland.pdf	15
Anlage-VT Verpflichtungserklärung Tariftreue und Mindestlohn.pdf	17
Vertragsunterlagen UKF	19
Lieferanten Code of ConductDE	19
20261019 EVB-IT digital Dienstvertrag neu Korrektur	27
Anlage- AVV (1)	41
20261019 Anlage Z - Zuschlagskriterien	57
Anlage AL Korrektur 14.07.2026	63
Anlage L-LV Managed Service LAN UKF final RG	71
Produkte/Leistungen	129
Eignungskriterien	133
Leistungskriterien	141
Anlagen	142

12.08.2026

{Bieterdaten: Name | Supplier.Name}
{Bieterdaten: Straße | Supplier.AddressStreet}
{Bieterdaten: PLZ und Ort | Supplier.AddressZipCodeCity}

Unser Zeichen: 20261019

Betreff: Aufforderung zur Abgabe eines Angebots

Sehr geehrte Damen und Herren,

das Universitätsklinikum Frankfurt – Anstalt des öffentlichen Rechts – schreibt im Namen und auf Rechnung von Universitätsklinikum Frankfurt 60590 Frankfurt am Main folgende Leistung aus:

Netzwerkbetrieb Managed Service

Offenes Verfahren (EU) (VgV)

Vertragsbeginn:

Leistungsbeginn:

Ende:

Anmerkungen: 60 Monate

Der Umfang der Leistung ergibt sich aus der Leistungsbeschreibung. Der Zuschlag wird auf das wirtschaftlichste Angebot erteilt.

I. Zuschlagskriterium

Wirtschaftlichstes Angebot
Berechnungsmethode: Freie Verhältniswahl Preis/Leistung
Gewichtung: 40%: 60%

Wertungsbereich	Gewichtung	Max. P.	Min. P.
Preis (Wertungssumme über 60 Monate)	40 %	40	0
Qualität – Übernahme, Transition, Implementierung und Ramp-up	15 %	15	0
Qualität – Managed Service, Monitoring, Reporting und Automatisierung	25 %	25	0
Qualität – Eingesetztes Betriebsteam (Qualifikation und Erfahrung)	10 %	10	0
Qualität – Exit und Providerwechsel	10 %	10	0
Gesamtwertungssumme	100 %	100	0

II. Verfahren

Nebenangebote sind nicht zugelassen

Es ist nur die Abgabe eines Hauptangebots zugelassen.

A. Fristen

Angebotsfrist: 19.08.2026 12:00:00 Uhr

Bindefrist: 14.09.2026

Frist für Bieterfragen: 16.07.2026 12:00 Uhr

B. Anlagen/Unterlagen, die im Vergabeverfahren zu beachten sind:

- Anlage-D Datenschutzerklärung
- Anlage-BEU Bewerbungsbedingungen EU
- Anlage-Z Zuschlagskriterien
- Lageplan (abzurufen unter: https://www.unimedizin-ff.m.de/fileadmin/redakteure/Presse/Lageplan/lageplan_ukf.pdf)

C. Elektronische Teilnahme

Bitte melden Sie sich auf der Bekanntmachungsplattform unter <https://portal.deutsche-e-vergabe.de> mit Ihrem Benutzernamen und Ihrem Passwort an.

Sofern Sie im System noch nicht registriert sind, können Sie dies auf der Plattform vornehmen. Die Registrierung ist kostenfrei. Anschließend können Sie auf der Startseite bspw. nach dem Titel des Verfahrens über die Direksuche als Suchbegriff suchen. Folgen Sie anschließend der Anleitung im System, um an dem Verfahren teilzunehmen.

D. Angebotsabgabe

Es werden nur elektronische Angebote in Schriftform akzeptiert!

Unterschriften: Durch Hochladen des Angebotes und die in der eVergabe hinterlegte Signatur gilt das Angebot als signiert abgegeben.

E. Bieterfragen & Kommunikation

Bieterfragen müssen bis spätestens 16.07.2026 12:00 Uhr eingegangen sein. Für später eingehende Fragen wird keine Beantwortung zugesichert.

Bieterfragen müssen unter "Nachrichten" im eVergabe-Bieterassistenten gestellt und dort geprüft werden.

Den Assistenten erreichen Sie unter <https://portal.deutsche-e-vergabe.de>. Fragen auf anderen Kommunikationswegen, wie telefonisch, schriftlich oder per E-Mail, werden nicht beantwortet.

Hinweis: Sie erhalten nach Beantwortung einer Bieterfrage eine Benachrichtigung per E-Mail. Alle Antworten müssen im Assistenten geprüft werden.

F. Vor-Ort-Besichtigung

Im Rahmen dieser Vergabe werden keine Objektbesichtigungen als erforderlich angesehen.

III. Bietergemeinschaft

Wird zur Leistungserbringung eine Bietergemeinschaft gebildet, ist die Anlage-EBG Eigenerklärung Bietergemeinschaft mit dem Angebot anzugeben und von jedem Mitglied der Bietergemeinschaft sind zusätzlich folgende Erklärung abzugeben:

- Anlage-BMWK Eigenerklärung Bezug zu Russland
- Anlage-VT Verpflichtungserklärung Tariftreue und Mindestlohn

Diese Dokumente sind gesondert von den dazu berechtigten Personen zu signieren.

IV. Nachunternehmer

Beabsichtigt der Bieter, Leistungen durch Nachunternehmer ausführen zu lassen, sind folgende Erklärungen und Nachweise abzugeben:

- Art und Umfang der Leistungen durch Nachunternehmer (Anlage-EN1, vom Bieter unterschrieben)
- Verpflichtungserklärung des Nachunternehmers (Anlage-EN2, vom Nachunternehmer unterschrieben).

Von allen Nachunternehmern sind nachfolgend aufgeführte Erklärungen und Nachweise mit dem Angebot einzureichen:

- Anlage-BMWK Eigenerklärung Bezug zu Russland
- Anlage-VT Verpflichtungserklärung Tariftreue und Mindestlohn

Die Einschaltung weiterer Nachunternehmer als der im Angebot benannten Nachunternehmer bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Der Bieter muss sicherstellen, dass ein Nachunternehmer die Leistungen nicht seinerseits ohne vorherige schriftliche Zustimmung des Auftraggebers weitervergibt.

Der Auftragnehmer ist verpflichtet,

- bei der Übertragung eines Unterauftrags nach wettbewerblichen Gesichtspunkten zu verfahren,
- dem Auftraggeber den Nachunternehmer zu benennen,
- dem Nachunternehmer insgesamt keine ungünstigeren Bedingungen – insbesondere hinsichtlich der Zahlungsweise und Sicherheitsleistungen – zu stellen, als zwischen ihm und dem Auftraggeber vereinbart sind.

Bei der Einholung von Angeboten für Unteraufträge sind regelmäßig kleine und mittlere Unternehmen angemessen zu beteiligen. Der Auftragnehmer hat sich ferner zu bemühen, Unteraufträge an kleine und mittlere Unternehmen in dem Umfang zu erteilen, wie er es mit der vertragsgemäßen Ausführung der Leistung vereinbaren kann.

V. Eignungsleihe

Sofern ein Bieter im Hinblick auf die erforderliche wirtschaftliche und finanzielle sowie die technische und berufliche Leistungsfähigkeit die Kapazitäten anderer Unternehmen in Anspruch nehmen will, wird im Rahmen der Eignungsprüfung überprüft, ob die Unternehmen, deren Kapazitäten der Bewerber oder Bieter für die Erfüllung bestimmter Eignungskriterien in Anspruch nehmen will, die entsprechenden Eignungskriterien erfüllen und ob Ausschlussgründe vorliegen.

Nimmt ein Bieter die Kapazitäten eines anderen Unternehmens im Hinblick auf die erforderliche wirtschaftliche und finanzielle Leistungsfähigkeit in Anspruch, so behält sich der Auftraggeber vor eine gemeinsame Haftung des Bieters und des anderen Unternehmens für die Auftragsausführung entsprechend dem Umfang der Eignungsleihe zu verlangen.

VI. Angebotsschreiben

Mit der Anlage-A Angebotsschreiben sind alle geforderten Anlagen und Nachweise abzugeben.

A. Unterlagen, die ggfs. ausgefüllt beigelegt / erstellt werden müssen:

- Anlage Produkte/Leistungen (Positionsteil; im Bietercockpit der eVergabe)
- Anlage Kriterienkatalog (im Bietercockpit der eVergabe)
- Anlage-P - Preisblatt
- Gültiges ISO 27001-Zertifikat
- Gültiges ISO 9001-Zertifikat
- Eigenerklärung EU/EWR-Datenverarbeitung und Subunternehmer
- Eigenerklärung CCNP Enterprise (Anzahl zertifizierter Mitarbeiter, min. 5)
- Eigenerklärung CCIE Enterprise Infrastructure (Anzahl + Name Technical Lead, min. 2)
- Eigenerklärung Business Continuity / Notbetrieb
- Konzepte gem. Anlage Z

- **bei Bietergemeinschaften:**
 - Anlage-EN 1 Eigenerklärung Nachunternehmereinsatz
 - Anlage-EN 2 Verpflichtungserklärung Nachunternehmer
 - Anlage-EBG Eigenerklärung Bietergemeinschaft
 - Anlage-BMWK bei Nachunternehmern + Bietergemeinschaft
 - Anlage-VT bei Nachunternehmern + Bietergemeinschaft

B. Unterlagen, die auf gesondertes Verlangen der Vergabestelle vorzulegen sind:

- Urkalkulation
- weitergehende Referenznachweise

C. Anlagen des Bieters

Es wird ausdrücklich darauf hingewiesen, dass alle dem Angebot beigefügten Anlagen Angebotsbestandteil sind. Dies gilt auch für Prospekte und Technische Datenblätter.

Falls es nicht ausdrücklich gefordert wird, ist die Abgabe von Prospekten, Broschüren oder Datenblättern nicht erwünscht und kann zum Ausschluss des Bieters führen.

Sofern Prospekte oder Datenblätter beigefügt werden, muss aus dem Prospekt oder dem Datenblatt eindeutig hervorgehen und vom Bieter markiert werden, welches Produkt und welche Produktkonfiguration oder Leistung angeboten wird.

Wird vom Bieter in den von ihm mit dem Angebot abgegebenen Anlagen auf Zertifizierungen/Nachweise verwiesen, sind diese ebenfalls als Anlagen dem Angebot beizufügen.

Werden vom Bieter eigene Allgemeine-, Besondere-, Zusätzliche oder Ergänzende Geschäftsbedingungen mit dem Angebot abgegeben oder in Angebotsanlagen auf diese verwiesen, ist das Angebot nicht beauftragungsfähig, da es unter einem nicht vorgesehenen Vorbehalt steht.

VII. Vertragsunterlagen

A. Unterlagen die bei Beauftragung Vertragsbestandteil werden:

- Anlagen/Unterlagen gemäß Abschnitt VI. A
- Leistungsbeschreibung/-verzeichnis, Pflichten-/Lastenheft
- Code of Conduct für Lieferanten (abzurufen unter: <https://www.unimedizin-ff.m.de/ueber-uns/lieferkettensorgfaltspflichtengesetz>)
- EVB-IT Vertrag
- Anlage -AVV Auftragsdatenverarbeitung (nach Zuschlag vom Auftragnehmer auszufüllen)

B. Skonto

Der Auftraggeber ist gemäß AEB berechtigt, bei Zahlung innerhalb von 21 Tagen (30 Tage netto) ab Rechnungseingang beim Auftraggeber ein Skonto in Höhe von 3 v.H. des Rechnungsbetrages abzuziehen.

Erfolgt die Leistung später, so gilt der Tag der ordnungsgemäßen Erfüllung des Auftrages.

Eine Nichtgewährung von den vorgenannten Skonti führt zum Ausschluss des Angebotes von der Wertung.

Wird ein höheres Skonto zu den vorgenannten Bedingungen angeboten, so gilt dies als vereinbart.

VIII. Schutzrechte

Der Auftragnehmer stellt den Auftraggeber auf eigene Kosten von allen Ansprüchen Dritter frei, die gegen den Auftraggeber wegen Verletzung von Schutzrechten an den angebotenen Geräten oder Dienstleistungen geltend gemacht werden.

IX. Verschwiegenheit

Der Bieter hat auch nach Beendigung des Vergabeverfahrens über die ihm bei seiner Tätigkeit bekannt gewordenen Informationen Verschwiegenheit zu bewahren. Er hat hierzu auch die mit der Erstellung des Angebotes beschäftigten Mitarbeiter und Nachunternehmer zu verpflichten. Der Auftraggeber behält sich vor, diesbezügliche Nachweise im Falle der beabsichtigten Auftragsvergabe zu verlangen.

X. Rechtsschutz

Behörde für Nachprüfung behaupteter Verstöße gegen Vergabebestimmungen (Vergabekammer gem. § 156 GWB): Vergabekammer des Landes Hessen beim Regierungspräsidium Darmstadt

Wilhelminenstraße 1–3 (Wilhelminenhof)

64283 Darmstadt

Kontakt ist per E-Mail unter vergabekammer@rpda.hessen.de

Mit freundlichen Grüßen,
Vergabeabteilung

Aufsichtsrat
Christoph Degen
(Vorsitzender)

Postanschrift
Universitätsklinikum Frankfurt
Theodor-Stern-Kai 7
60590 Frankfurt a. M.

Frankfurter Sparkasse
IBAN: DE32 5005 0201 0000
3799 99
BIC: HELADEF1822

Postbank Frankfurt
IBAN: DE14 5001 0060 0000
7606 03
BIC: PBNKDEFF

Bewerbungsbedingungen für die Vergabe von Leistungen

Das Vergabeverfahren erfolgt nach der Vergabeverordnung (VgV).

1 Mitteilung von Unklarheiten in den Vergabeunterlagen

Enthalten die Vergabeunterlagen nach Auffassung des Unternehmens Unklarheiten, Unvollständigkeiten oder Fehler, so hat es unverzüglich die Vergabestelle vor Angebotsabgabe in Textform darauf hinzuweisen.

2 Unzulässige Wettbewerbsbeschränkungen

Angebote von Bietern, die sich im Zusammenhang mit diesem Vergabeverfahren an einer unzulässigen Wettbewerbsbeschränkung beteiligen, werden ausgeschlossen.

Zur Bekämpfung von Wettbewerbsbeschränkungen hat der Bieter auf Verlangen Auskünfte darüber zu geben, ob und auf welche Art er wirtschaftlich und rechtlich mit Unternehmen verbunden ist.

3 Angebot

3.1 Das Angebot ist in deutscher Sprache abzufassen.

3.2 Für das Angebot sind die von der Vergabestelle vorgegebenen Vordrucke zu verwenden. Das Angebot ist bis zu dem von der Vergabestelle angegebenen Ablauf der Angebotsfrist einzureichen. Ein nicht form- oder fristgerecht eingereichtes Angebot wird ausgeschlossen.

3.3 Eine selbst gefertigte Abschrift oder Kurzfassung des Leistungsverzeichnisses ist zulässig.

Die von der Vergabestelle vorgegebene Langfassung des Leistungsverzeichnisses ist allein verbindlich.

3.4 Unterlagen, die von der Vergabestelle nach Angebotsabgabe verlangt werden, sind zu dem von der Vergabestelle bestimmten Zeitpunkt einzureichen.

3.5 Alle Eintragungen müssen dokumentenecht sein.

3.6 Ein Bieter, der in seinem Angebot die von ihm tatsächlich für einzelne Leistungspositionen geforderten Einheitspreise auf verschiedene Einheitspreise anderer Leistungspositionen verteilt, benennt nicht die von ihm geforderten Preise. Deshalb werden Angebote, bei denen der Bieter die Einheitspreise einzelner Leistungspositionen in „Mischkalkulationen“ auf andere Leistungspositionen umlegt, von der Wertung ausgeschlossen.

3.7 Alle Preise sind in Euro mit höchstens drei Nachkommastellen anzugeben.

Die Preise (Einheitspreise, Pauschalpreise, Verrechnungssätze usw.) sind ohne Umsatzsteuer anzugeben. Der Umsatzsteuerbetrag ist unter Zugrundelegung des geltenden Steuersatzes am Schluss des Angebotes hinzuzufügen.

Es werden nur Preisnachlässe gewertet, die

- ohne Bedingungen als Vomhundertsatz auf die Abrechnungssumme gewährt werden und

- an der im Angebotsschreiben bezeichneten Stelle aufgeführt sind.

Nicht zu wertende Preisnachlässe bleiben Inhalt des Angebotes und werden im Fall der Auftragserteilung Vertragsinhalt.

4 Nebenangebote

4.1 Nebenangebote müssen die geforderten Mindestanforderungen erfüllen; dies ist mit Angebotsabgabe nachzuweisen.

4.2 Der Bieter hat die in Nebenangeboten enthaltenen Leistungen eindeutig und erschöpfend zu beschreiben; die Gliederung des Leistungsverzeichnisses ist, soweit möglich, beizubehalten.

Nebenangebote müssen alle Leistungen umfassen, die zu einer einwandfreien Ausführung der Leistung erforderlich sind.

Soweit der Bieter eine Leistung anbietet, deren Ausführung nicht in den Vergabeunterlagen geregelt ist, hat er im Angebot entsprechende Angaben über Ausführung und Beschaffenheit dieser Leistung zu machen.

- 4.3 Nebenangebote sind, soweit sie Teilleistungen (Positionen) des Leistungsverzeichnisses beeinflussen (ändern, ersetzen, entfallen lassen, zusätzlich erfordern), nach Mengenansätzen und Einzelpreisen aufzugliedern (auch bei Vergütung durch Pauschalsumme).
- 4.4 Nebenangebote, die den Nummern 4.1 bis 4.3 nicht entsprechen, werden von der Wertung ausgeschlossen.

5 Bietergemeinschaften

- 5.1 Die Bietergemeinschaft hat mit ihrem Angebot eine Erklärung aller Mitglieder in Textform abzugeben,
- in der die Bildung einer Arbeitsgemeinschaft im Auftragsfall erklärt ist,
 - in der alle Mitglieder aufgeführt sind und der für die Durchführung des Vertrags bevollmächtigte Vertreter bezeichnet ist,
 - dass der bevollmächtigte Vertreter die Mitglieder gegenüber dem Auftraggeber rechtsverbindlich vertritt,
 - dass alle Mitglieder als Gesamtschuldner haften.
- Auf Verlangen der Vergabestelle ist eine von allen Mitgliedern unterzeichnete bzw. fortgeschritten oder qualifiziert signierte Erklärung abzugeben.
- 5.2 Sofern nicht im offenen Verfahren ausgeschrieben wird, werden Angebote von Bietergemeinschaften, die sich erst nach der Aufforderung zur Angebotsabgabe aus aufgeforderten Unternehmen gebildet haben, nicht zugelassen.

6 Kapazitäten anderer Unternehmen (Unteraufträge, Eignungsleihe)

Beabsichtigt der Bieter, Teile der Leistung von anderen Unternehmen ausführen zu lassen oder sich bei der Erfüllung eines Auftrages im Hinblick auf die erforderliche wirtschaftliche, finanzielle, technische oder berufliche Leistungsfähigkeit anderer Unternehmen zu bedienen, so muss er die hierfür vorgesehenen Leistungen/Kapazitäten in seinem Angebot benennen. Der Bieter hat auf gesondertes Verlangen der Vergabestelle zu einem von ihr bestimmten Zeitpunkt nachzuweisen, dass ihm die erforderlichen Kapazitäten der anderen Unternehmen zur Verfügung stehen und diese Unternehmen geeignet sind. Er hat den Namen, den gesetzlichen Vertreter sowie die Kontaktdaten dieser Unternehmen anzugeben und entsprechende Verpflichtungserklärungen dieser Unternehmen vorzulegen.

Nimmt der Bieter in Hinblick auf die Kriterien für die wirtschaftliche und finanzielle Leistungsfähigkeit im Rahmen einer Eignungsleihe die Kapazitäten anderer Unternehmen in Anspruch, müssen diese gemeinsam für die Auftragsausführung haften; die Haftungserklärung ist gleichzeitig mit der Verpflichtungserklärung abzugeben.

Der Bieter hat andere Unternehmen, bei denen Ausschlussgründe vorliegen oder die das entsprechende Eignungskriterium nicht erfüllen, innerhalb einer von der Vergabestelle gesetzten Frist zu ersetzen.

7 Eignung

Unternehmen haben als Nachweis der Eignung für die zu vergebende Leistung mit dem Angebot

- **Entweder** die in der Auftragsbekanntmachung oder der Aufforderung zur Interessensbestätigung angegebenen Unterlagen (Eigenerklärungen, Angaben, Bescheinigungen und sonstige Nachweise)
- **Oder** eine Einheitliche Europäische Eigenerklärung (EEE) als vorläufigen Nachweis vorzulegen.

Bei Einsatz von anderen Unternehmen gemäß Nummer 6 sind auf gesondertes Verlangen die Unterlagen/die EEE auch für diese abzugeben.

Gelangt das Angebot in die engere Wahl, sind Eigenerklärungen (auch die der benannten anderen Unternehmen) auf gesondertes Verlangen durch Vorlage der genannten Bescheinigungen zuständiger Stellen zu bestätigen. Bescheinigungen, die nicht in deutscher Sprache abgefasst sind, ist eine Übersetzung in die deutsche Sprache beizufügen.

Die Verpflichtung zur Vorlage von Eigenerklärungen und Bescheinigungen entfällt, soweit die Eignung (Bieter und benannte andere Unternehmen) bereits im Teilnahmewettbewerb nachgewiesen ist.

Universitätsmedizin Frankfurt
Vergabenummer: 20261019
Vergabeverfahren: Netzwerkbetrieb Managed Service

Information nach Art. 13 Datenschutz-Grundverordnung (DSGVO)

Information nach Art. 13 DSGVO

Vertrauen ist wichtig, besonders wenn es um Ihre Daten geht. Aus diesem Grund erachten wir es als unsere Verpflichtung, nur die Daten zu erheben, welche unbedingt erforderlich sind, sowie die Daten mit der gebotenen Sorgfalt zu verwalten und vor Missbräuchen zu schützen.

Die Universitätsmedizin Frankfurt hält sich strikt an die datenschutzrechtlichen Vorschriften bei der Erhebung und Verarbeitung Ihrer Daten.

Nachstehend finden Sie Informationen zur Verarbeitung Ihrer Daten und den Ihnen zukommenden Rechten:

1. Name und Kontaktdaten des/der Verantwortlichen

Universitätsmedizin Frankfurt
Theodor-Stern-Kai 7
60596 Frankfurt am Main
Telefon: +49 69 63 01-0
Fax: +49 69 6301-63 01

E-Mail: info@unimedizin-ffm.de
Internet: www.unimedizin-ffm.de

2. Kontaktdaten der/des Datenschutzbeauftragten (gemäss Art. 37 DSGVO)

Datenschutzbeauftragte(r) der Universitätsmedizin Frankfurt
Theodor-Stern-Kai 7
60596 Frankfurt am Main

Telefon: +49 69 63 01-7235
E-Mail: datenschutz@unimedizin-ffm.de

3. Kategorien der erhobenen personenbezogenen Daten, Zwecke und Rechtsgrundlagen der Verarbeitung

Im Vergabeverfahren sind personenbezogene Daten, insbesondere bei der Eignungsprüfung von Bedeutung, etwa wenn die Bieter aufgefordert werden, Referenzen mit Lebensläufen, Namen, Adressen und Fotos ihrer Mitarbeiter vorzulegen. Auch Studien- und Ausbildungsnachweise sind personenbezogene Daten, welche im Rahmen des Verfahrens verarbeitet werden können.

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene einwilligt.

Nach Art. 6 Abs. 1 b) DSGVO ist die Datenverarbeitung zulässig, wenn sie zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Die Datenverarbeitung ist zudem nach Art. 6 Abs. 1 c) DSGVO zulässig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welcher der Verantwortliche unterliegt. Gem. Art. 6 Abs. 1 a) DSGVO ist die Datenverarbeitung zulässig, wenn sie auf einer Einwilligung beruht.

Da wir als Vergabestelle nach dem Vergaberecht verpflichtet sind, die Eignung unter Verarbeitung von personenbezogenen Daten zu prüfen, ist dies nach den vorgenannten Regelungen zulässig.

Zudem kommt eine Verarbeitung aufgrund einer konkludenten Einwilligung in Betracht, wenn die Bieter und deren Beschäftigte personenbezogene Daten im Rahmen der Bewerbung selbst zur Verfügung stellen.

4. Dauer der Speicherung der personenbezogenen Daten

Ihre Daten werden nach der Erhebung so lange gespeichert, wie dies

- unter Beachtung der gesetzlichen Aufbewahrungsfristen gemäß §8 Abs 4 VgV bzw. §6 Abs. 2 UVgO erforderlich ist.

5. Betroffenenrechte

Nach der EU-Datenschutz-Grundverordnung stehen Ihnen folgende Rechte zu:

- (i) Auskunft zu erhalten über die verarbeiteten personenbezogenen Daten bzw. deren Kategorien, die Verarbeitungszwecke, die Kategorien von Empfängern, gegenüber denen Ihre Daten offengelegt wurden oder werden, die Absicht, Daten an ein Drittland oder eine internationale Organisation zu übermitteln einschliesslich dafür geeigneter Garan-

tien, die geplante Speicherdauer, das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch, das Bestehen eines Beschwerderechts, die Herkunft Ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschliesslich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten,

- (ii) die Berichtigung, Ergänzung, oder das Löschen Ihrer personenbezogenen Daten, die falsch sind oder nicht rechtskonform verarbeitet werden, zu verlangen,
- (iii) von uns zu verlangen, die Verarbeitung Ihrer personenbezogenen Daten einzuschränken,
- (iv) unter bestimmten Umständen der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen oder die für das Verarbeiten zuvor gegebene Einwilligung zu widerrufen,
- (v) Ihre personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen,
- (vi) bei der zuständigen Datenschutzaufsichtsbehörde Beschwerde zu erheben.

6. Widerrufsrecht bei Einwilligung

Wenn Sie in die Verarbeitung durch eine entsprechende Erklärung eingewilligt haben, können Sie die Einwilligung jederzeit für die Zukunft widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.

Möchten Sie von Ihrem Widerrufsrecht Gebrauch machen, teilen Sie dies per E-Mail an datenschutz@unimedizin-ffm.de mit.

Name bzw. Firmenbezeichnung des Bieters

Zuständige Sachbearbeitung beim Bieter

Telefon

E-Mail Adresse

Geschäftszeichen des Bieters

Universitätsklinikum Frankfurt

Anstalt des öffentlichen Rechts

Abteilung 3.3 Zentrale Vergabe

Theodor-Stern-Kai 7

D-60590 Frankfurt

Vergabenummer der Vergabestelle
20261019

Angebot

Lieferung/Leistung

Netzwerkbetrieb Managed Service

Sehr geehrte Damen und Herren,

die Ausführung der beschriebenen Leistung wird hiermit zu den eingesetzten Preisen angeboten.

Wir halten uns bis zum Ende der Bindefrist an dieses Angebot gebunden.

Dem Angebot liegen die in der o. g. Aufforderung zur Abgabe eines Angebotes übersandten
Bewerbungsbedingungen sowie die sonstigen dort genannten Bedingungen zugrunde.

Die Angebotsendsumme in Euro gemäß
Leistungsbeschreibung einschl. Umsatzsteuer beträgt:

Preisnachlass in % ohne Bedingung auf die Abrechnungssumme
für das Angebot:

Skonto:

Der Auftraggeber ist berechtigt Skonto abzuziehen. Die Fristen und Skonti ergeben sich aus
den Vergabeunterlagen, die Angebotsbestandteil sind.

Die Skontofrist beginnt mit dem Tag des Eingangs der prüffähigen Rechnung beim
Auftraggeber.

Bestandteil meines/unseres Angebotes sind sämtliche Vertragsbedingungen, inklusive der VOL/A, welche die Auftraggeberin den Vergabeunterlagen beigefügt hat.

Wir sind uns bewusst, dass wissentlich falsche Erklärungen den Ausschluss von dieser und von weiteren Ausschreibungen zur Folge haben können.

Wir erklären, dass:

ich/wir die Leistungen, die nicht im Verzeichnis der Leistungen anderer Unternehmen aufgeführt sind (Anlage-EN1), im eigenen Betrieb ausführen werden.

ich/wir die gewerberechtlichen Voraussetzungen für die Ausführung der angebotenen Leistung erfülle(n).

ich/wir den Wortlaut der vom Auftraggeber verfassten Langfassung des Leistungsverzeichnisses als alleinverbindlich anerkenne(n),

mir/uns zugegangene Änderungen der Vergabeunterlagen Gegenstand meines/unseres Angebotes sind.

das vom Auftraggeber vorgeschlagene Produkt Inhalt meines/unseres Angebotes ist, wenn Teilleistungsbeschreibungen des Auftraggebers den Zusatz „oder gleichwertig“ enthalten und von mir/uns keine Produktangaben (Hersteller- und Typbezeichnungen) eingetragen wurden.

falls von mir/uns mehrere Nebenangebote abgegeben wurden, mein/unser Angebot auch die Kumulation der Nebenangebote, die sich nicht gegenseitig ausschließen, umfasst.

Hinweis: Durch Hochladen des Angebotes und die in der eVergabe hinterlegte Signatur gilt das Angebot als signiert abgegeben.

Anlagen: siehe nächste Seite

[illegible]

Anlage-EN 1 Eigenerklärung Nachunternehmen

Bieter	Vergabenummer	Datum
	20261019	
Projekt		
Leistung Netzwerkbetrieb Managed Service		

Ergänzung des Angebotsschreibens

Verzeichnis über Art und Umfang der Leistungen, für die sich der Bieter der Kapazitäten anderer Unternehmen bedienen wird

Zur Ausführung der im Angebot enthaltenen Leistungen benenne ich Art und Umfang der Teilleistungen, für die ich mich/wir uns anderer Unternehmen bedienen werde(n).

OZ/Leistungsbereich	Beschreibung der Teilleistungen / Firma des Nachunternehmers

In Hinsicht auf meine/unsere wirtschaftliche und finanzielle Leistungsfähigkeit	
Name des Unternehmens	Angabe zu der von diesem Unternehmen überlassenen Eignung

Anlage-EN2 Verpflichtungserklärung Nachunternehmen

Bewerber/Bieter	Vergabenummer	Datum
	20261019	
Projekt		
Leistung Netzwerkbetrieb Managed Service		

Name, gesetzlicher Vertreter, Kontaktdaten des sich verpflichtenden Unternehmens
--

Verpflichtungserklärung anderer Unternehmen

Ich/Wir verpflichte(n) mich/uns gegenüber dem Auftraggeber, im Falle der Auftragsvergabe an den o.g. Bewerber/Bieter diesem mit den erforderlichen Kapazitäten meines/unseres Unternehmens für den/die nachfolgenden Leistungsbereich(e) zur Verfügung zu stehen.

OZ/Leistungsbereich	Beschreibung der (Teil)Leistungen

(Ort, Datum, Unterschrift)

- ☐ Der Bewerber bzw. Bieter nimmt zum Nachweis seiner Eignung die wirtschaftliche und finanzielle Leistungsfähigkeit meines/unseres Unternehmens in Anspruch. Ich/Wir verpflichte(n) mich/uns gegenüber dem Auftraggeber, im Falle der Auftragsvergabe an den o.g. Bewerber/Bieter mit diesem gemeinsam für die Auftragsausführung zu haften.

(Ort, Datum, Unterschrift)

Anmerkung: Sofern Verpflichtungserklärungen in Kopie oder als Telefax vorgelegt werden, behält sich die Vergabestelle vor, die Originale zu verlangen.

Anlage-EBG Erklärung Bietergemeinschaft

Bezeichnung der Leistung:

Maßnahmennummer	Projekt
Vergabenummer	Leistung
20261019	Netzwerkbetrieb Managed Service

Erklärung der Bieter- /Arbeitsgemeinschaft

Wir, die nachstehend aufgeführten Unternehmen einer Bietergemeinschaft,

Bevollmächtigter Vertreter

Mitglied _____

USt-ID: _____

Weitere Mitglieder

Mitglied _____

USt-ID: _____

Mitglied _____

USt-ID: _____

Mitglied _____

USt-ID: _____

beschließen, im Falle der Auftragserteilung eine Arbeitsgemeinschaft zu bilden und erklären¹, dass der bevollmächtigte Vertreter die Mitglieder gegenüber dem Auftraggeber rechtsverbindlich vertritt und alle Mitglieder als Gesamtschuldner haften.

Ort Datum Unterschrift

Ort Datum Unterschrift

Ort Datum Unterschrift

Ort Datum Unterschrift

¹ Die Bietergemeinschaft hat mit ihrem Angebot eine Erklärung aller Mitglieder in Textform abzugeben, Auf Verlangen der Vergabestelle ist eine von allen Mitgliedern unterzeichnete bzw. fortgeschritten oder qualifiziert signierte Erklärung abzugeben.

- Anlage zum BMWK-Rundschreiben vom 14.04.2022 -

Eigenerklärung

(von allen Bewerbern / Bieter / allen Mitgliedern von Bewerber- bzw. Bietergemeinschaften)

Bezeichnung des Vergabeverfahrens / Auftrags:

Geschäftszeichen des Auftraggebers:

20261019

Die nachfolgende Erklärung gebe/n ich/wir verbindlich ab (ggf. zugleich in Vertretung für die lt. Teilnahmeantrag / Angebot Vertretenen auch für diese):

1. Der / die **Bewerber / Bieter** gehört / gehören nicht zu den

in **Artikel 5 k)** Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren,

genannten Personen oder Unternehmen, die einen Bezug zu Russland im Sinne der Vorschrift aufweisen,

- a) **durch die russische Staatsangehörigkeit des Bewerbers/Bieters oder die Niederlassung des Bewerbers/Bieters in Russland,**
- b) **durch die Beteiligung einer natürlichen Person oder eines Unternehmens, auf die eines der Kriterien nach Buchstabe a zutrifft, am Bewerber/Bieter über das Halten von Anteilen im Umfang von mehr als 50%,**
- c) **durch das Handeln der Bewerber/Bieter im Namen oder auf Anweisung von Personen oder Unternehmen, auf die die Kriterien der Buchstaben a und/oder b zutrifft.**

2. Die am Auftrag als **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, beteiligten Unternehmen, auf die mehr als 10 % des Auftragswerts entfällt, gehören ebenfalls nicht zu dem in der Vorschrift genannten Personenkreis mit einem Bezug zu Russland im Sinne der Vorschrift.

3. Es wird bestätigt und sichergestellt, dass auch während der Vertragslaufzeit keine als **Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden**, beteiligten Unternehmen eingesetzt werden, auf die mehr als 10 % des Auftragswerts entfällt.

_____, den _____

Unterschriften (bei elektronischer Übermittlung: Name der erklärenden Person)

Artikel 5k der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 lautet wie folgt:

(1) Es ist verboten, öffentliche Aufträge oder Konzessionen, die in den Anwendungsbereich der Richtlinien über die öffentliche Auftragsvergabe sowie unter Artikel 10 Absatz 1, Absatz 3, Absatz 6 Buchstaben a bis e, Absatz 8, Absatz 9 und Absatz 10 und die Artikel 11, 12, 13 und 14 der Richtlinie 2014/23/EU, unter die Artikel 7 und 8, Artikel 10 Buchstaben b bis f und h bis j der Richtlinie 2014/24/EU, unter Artikel 18, Artikel 21 Buchstaben b bis e und g bis i, Artikel 29 und Artikel 30 der Richtlinie 2014/25/EU und unter Artikel 13 Buchstaben a bis d, f bis h und j der Richtlinie 2009/81/EG fallen, an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen:

a) russische Staatsangehörige oder in Russland niedergelassene natürliche oder juristische Personen, Organisationen oder Einrichtungen,

b) juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50 % unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, oder

c) natürliche oder juristische Personen, Organisationen oder Einrichtungen, die im Namen oder auf Anweisung einer der unter Buchstabe a oder b genannten Organisationen handeln,

auch solche, auf die mehr als 10 % des Auftragswerts entfällt, Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Sinne der Richtlinien über die öffentliche Auftragsvergabe in Anspruch genommen werden.

(2) Abweichend von Absatz 1 können die zuständigen Behörden die Vergabe oder die Fortsetzung der Erfüllung von Verträgen genehmigen, die bestimmt sind für

a) den Betrieb ziviler nuklearer Kapazitäten, ihre Instandhaltung, ihre Stilllegung, die Entsorgung ihrer radioaktiven Abfälle, ihre Versorgung mit und die Wiederaufbereitung von Brennelementen und die Weiterführung der Planung, des Baus und die Abnahmetests für die Indienststellung ziviler Atomanlagen und ihre Sicherheit sowie die Lieferung von Ausgangsstoffen zur Herstellung medizinischer Radioisotope und ähnlicher medizinischer Anwendungen, kritischer Technologien zur radiologischen Umweltüberwachung sowie für die zivile nukleare Zusammenarbeit, insbesondere im Bereich Forschung und Entwicklung,

b) die zwischenstaatliche Zusammenarbeit bei Raumfahrtprogrammen,

c) die Bereitstellung unbedingt notwendiger Güter oder Dienstleistungen, wenn sie ausschließlich oder nur in ausreichender Menge von den in Absatz 1 genannten Personen bereitgestellt werden können,

d) die Tätigkeit der diplomatischen und konsularischen Vertretungen der Union und der Mitgliedstaaten in Russland, einschließlich Delegationen, Botschaften und Missionen, oder internationaler Organisationen in Russland, die nach dem Völkerrecht Immunität genießen.

e) den Kauf, die Einfuhr oder die Beförderung von Erdgas und Erdöl, einschließlich raffinierter Erdölerzeugnisse, sowie von Titan, Aluminium, Kupfer, Nickel, Palladium und Eisenerz aus oder durch Russland in die Union, oder

f) den Kauf, die Einfuhr oder die Beförderung von Kohle und anderen festen fossilen Brennstoffen, die in Anhang XXII aufgeführt sind, bis 10. August 2022.

(3) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Artikel erteilte Genehmigung innerhalb von zwei Wochen nach deren Erteilung.

(4) Die Verbote gemäß Absatz 1 gelten nicht für die Erfüllung — bis zum 10. Oktober 2022 — von Verträgen, die vor dem 9. April 2022 geschlossen wurden.

(Name und Anschrift des Bieters)

Vergabenummer: 20261019

Verpflichtungserklärung zu Tariftreue und Mindestentgelt bei öffentlichen Aufträgen nach dem Hessischen Vergabe- und Tariftreuegesetz (HVTG) vom 19. Dezember 2014, GVBl. S. 354

Es wird darauf hingewiesen, dass sich die Verpflichtungserklärung zu Tariftreue und Mindestentgelt entsprechend den Vorgaben der §§ 4 und 6 des Hessischen Vergabe- und Tariftreuegesetzes (HVTG) zur Zahlung des Mindestlohns gemäß § 20 des Mindestlohngesetzes (MiLoG) bzw. des Tariflohns nach dem Arbeitnehmer-Entsendegesetz (AEntG) nicht auf Beschäftigte bezieht, die bei einem Bieter oder Nachunternehmer im EU-Ausland beschäftigt sind und die Leistung im EU-Ausland erbringen.

Nachfolgende Erklärung ist zu unterschreiben und mit dem Angebot abzugeben.

Ich/Wir erkläre/n:

1. Ich/wir nehme/n zur Kenntnis, dass ich/wir gemäß § 4 Abs. 1 HVTG die für mich/uns geltenden gesetzlichen, aufgrund eines Gesetzes festgesetzten und unmittelbar geltenden tarifvertraglichen Leistungen zu gewähren habe/n. Ich/wir nehme/n weiterhin zur Kenntnis, dass bei Vorliegen von Anhaltspunkten dafür, dass gegen diese Regelung verstoßen wird, auf Anforderung dem öffentlichen Auftraggeber oder dem Besteller die Einhaltung dieser Verpflichtung nachzuweisen ist.
 2. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 2 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung diejenigen Arbeitsbedingungen einschließlich des Entgelts zu gewähren, die nach Art und Höhe mindestens den Vorgaben desjenigen Tarifvertrags entsprechen, an den mein/unser Unternehmen aufgrund des AEntG gebunden ist.
 3. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 3 und § 6 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung ein Entgelt zu zahlen, das den Vorgaben des MiLoG entspricht. Im Falle der Auftragsausführung durch Nachunternehmer oder Verleihunternehmen sind im Angebot, soweit diese bereits bei Angebotsabgabe bekannt sind, spätestens jedoch vor Beginn der Ausführung der Leistung durch das Nachunternehmen oder Verleihunternehmen die entsprechenden Erklärungen in Textform abzugeben und vorzulegen.
- Die Erklärung kann entfallen, soweit sie bereits in einem Präqualifizierungsregister hinterlegt ist.

- Die Einhaltung der nach Bundesrecht oder aufgrund von Bundesrecht für mich/uns geltenden Regelungen von besonders festgesetzten Mindestentgelten (Mindestlohn) als Mindeststandard im Angebot entfällt, soweit nach § 4 HVTG Tariftreue gefordert werden kann und die danach maßgebliche tarifliche Regelung für die Beschäftigten günstiger ist als die für sie nach Bundesrecht geltenden Bestimmungen.
- 4. Ich/wir erkläre/n, dass ich/wir nicht wegen eines Verstoßes gegen § 21 MiLoG (Bußgeldvorschriften) mit einer Geldbuße von wenigstens 2.500 Euro belegt worden bin/sind und damit nicht die Voraussetzungen für einen Ausschluss von der Auftragsvergabe nach § 19 Abs. 1 und 3 MiLoG vorliegen.
- 5. Ich/wir verpflichte/n mich/uns für den Fall der Ausführung vertraglich übernommener Leistungen durch Nachunternehmen, die Erfüllung der Verpflichtungen nach den §§ 4 und 6 HVTG durch die Nachunternehmen sicherzustellen und dem öffentlichen Auftraggeber Tariftreue- und sonstige Verpflichtungs- sowie Mindestlohnerklärungen der Nachunternehmen nach Auftragserteilung, spätestens vor Beginn der Ausführung der Leistung durch das Nachunternehmen, vorzulegen. Gleiches gilt, wenn ich/wir oder ein beauftragtes Nachunternehmen zur Ausführung des Auftrags Arbeitskräfte eines Verleihunternehmens einsetze(n)/einsetzt. Diese Verpflichtung gilt entsprechend auch für alle weiteren Nachunternehmen und Verleihunternehmen.

Ort/Datum, Firma des Unternehmens, Name der natürlichen Person, die unterschriftsbefugt ist



UNIVERSITÄTSKLINIKUM



CODE OF CONDUCT

für Lieferanten des
Universitätsklinikum Frankfurt



Markus Jones, Prof. Dr. Jürgen Graf, Birgit Roelfsema, Prof. Dr. Stefan Zeuzem (v.l.)

I. Einleitung

Als Maximalversorger in Deutschland, vor allem aber im Rhein/Main-Gebiet, ist sich das Universitätsklinikum seiner Verantwortung gegenüber seinen Patientinnen und Patienten, gegenüber seinen Beschäftigten und gegenüber seinem Umfeld, explizit der Umwelt bewusst. Das Universitätsklinikum Frankfurt bekennt sich zur Einhaltung der Menschenrechte und zum Schutz der Umwelt. Es ist das erklärte Ziel der Unternehmensleitung, die Menschenrechte und die Umwelt entlang der gesamten Wertschöpfungskette zu achten, zu schützen und zu fördern.

Ebenso erwarten wir die Einhaltung der Menschenrechte und umweltbezogener Schutzpflichten von unseren Lieferanten.

Dieser Lieferanten Code of Conduct stützt sich auf nationale Gesetze und Vorgaben sowie auf internationale Übereinkommen.

Prof. Dr. Jürgen Graf
*Ärztlicher Direktor und
Vorstandsvorsitzender*

Markus Jones
*Kaufmännischer Direktor und
stellvertretender Vorstandsvorsitzender*

Birgit Roelfsema
Pflegedirektorin

Prof. Dr. Stefan Zeuzem
Dekan

INHALT

I. Einleitung	01
II. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt	04
III. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt	08
IV. Kenntnisnahme und Einverständnis des Lieferanten	08



II. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt

1. Menschenrechtsbezogene Verantwortung

1.1 Menschenrechte



Der Lieferant respektiert die persönliche Würde, Privatsphäre und die Menschenrechte eines jeden. Auf den Schutz der international anerkannten Menschenrechte ist angemessen hinzuwirken. Die Mitwirkung an Menschenrechtsverletzung ist durch den Lieferanten zu verhindern.

1.2 Verbot von Kinderarbeit



In keiner Phase der Produktion darf Kinderarbeit eingesetzt werden. Die Lieferanten sind aufgefordert, sich an die Empfehlungen aus den ILO-Konventionen zum Mindestalter für die Beschäftigung von Kindern zu halten. Demnach soll das Alter nicht geringer sein als das Alter, mit dem die allgemeine Schulpflicht endet und in jedem Fall nicht unter 15 Jahre.

1.3 Ausschluss von Zwangsarbeit



Es darf keine Zwangsarbeit, Sklavenarbeit oder derart vergleichbare Arbeit eingesetzt werden. Jede Arbeit muss freiwillig sein und die Mitarbeitenden müssen jederzeit die Arbeit oder das Beschäftigungsverhältnis beenden können. Außerdem darf keine inakzeptable Behandlung von Arbeitskräften, wie etwas psychische Härte, sexuelle und persönliche Belästigung stattfinden.

1.4 Einhaltung von angemessenem Arbeits- und Gesundheitsschutz



Der Lieferant sorgt für angemessene Sicherheitsmaßnahmen zum wirksamen Schutz seiner Beschäftigten vor Unfällen, chemischen, biologischen und physikalischen Gefahren sowie Berufskrankheiten, einschließlich Mitarbeiterunterweisungen und persönlicher Schutzausrüstung. Der Lieferant identifiziert und verhindert



wirksam relevante Risiken und Notfallsituationen am Arbeitsplatz, in der öffentlichen Umgebung und in den vom Unternehmen zur Verfügung gestellten Wohnräumen und stellt geeignete Notfallpläne, regelmäßige Sicherheitsschulungen und Reaktionsverfahren sicher.

1.5 Einhaltung der Vereinigungsfreiheit / Koalitionsfreiheit



Der Lieferant respektiert das Recht der Arbeitskräfte auf Vereinigungsfreiheit, auf Beitritt zu Gewerkschaften, auf Anruf der Arbeitskräftevertretung oder auf Mitgliedschaft in Betriebsräten/Personalräten in Übereinstimmung mit den vor Ort geltenden Gesetzen. Den Arbeitskräften muss es möglich sein, mit der Unternehmensleitung offen und ohne Angst vor Repressalien oder Belästigung zu kommunizieren.

1.6 Gleichbehandlung in der Beschäftigung



Die Diskriminierung von Beschäftigten in jeglicher Form ist unzulässig. Dies gilt z.B. für Benachteiligungen aufgrund von Geschlecht, Rasse, Kaste, Hautfarbe, Behinderung, politischer Überzeugung, Herkunft, Religion, Alter, Schwangerschaft oder sexueller Orientierung. Die persönliche Würde, Privatsphäre und Persönlichkeitsrechte jedes Einzelnen werden respektiert. Der Lieferant fördert die Chancengleichheit am Arbeitsplatz und die Gleichbehandlung seiner Mitarbeiter unabhängig von Hautfarbe, Nationalität, sozialer Herkunft, möglicher Behinderung, sexueller Orientierung, politischer oder religiöser Überzeugung sowie Geschlecht und Alter.



1.7 Faire Entlohnung



Der Lieferant vergütet seine Beschäftigten angemessen und gewährleistet die Zahlung der gesetzlich festgelegten nationalen Mindestlöhne. Die Arbeitszeiten haben den geltenden Gesetzen oder den Branchenstandards zu entsprechen.

1.8 Schutz der natürlichen Lebensgrundlagen

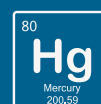


Der Lieferant hat schädliche Bodenveränderungen, Gewässer- und Luftverunreinigungen, Lärmemissionen sowie übermäßiger Wasserverbrauch zu unterlassen, wenn dadurch die Gesundheit von Personen schädigt, die natürliche Grundlage zur Produktion von Nahrung erheblich beeinträchtigt wird oder der Zugang von Personen zu Trinkwasser bzw. Sanitäranlagen verhindert wird.

Der Lieferant darf nicht unter Verstoß gegen legitime Rechte Land, Wälder oder Gewässer entziehen, deren Nutzung die Lebensgrundlage von Personen sichert.

2. Umweltschutzbezogene Verantwortung

2.1 Verbote im Kontext von Quecksilber



Die Verwendung von Quecksilber hat lediglich unter Beachtung der Verbote bzw. im Einklang mit dem Übereinkommen von Minamata in seiner aktuellen Fassung zu erfolgen.

2.2 Persistente organische Schadstoffe



Die Verwendung von persistenten organischen Schadstoffen hat lediglich unter Beachtung der Verbote bzw. im Einklang mit dem Stockholmer Übereinkommen in seiner aktuellen Fassung zu erfolgen.

2.3 Gefahrenabfall und Abfallentsorgung



Im Zusammenhang mit Festabfall hat der Lieferant einer systematischen Herangehensweise zu folgen was die Ermittlung, die Handhabung, Reduktion, verantwortungsvolle Entsorgungen bzw. Recycling dessen anbelangt. Des Weiteren sind entsprechende Verbote hinsichtlich der Ausfuhr von gefährlichen Abfällen gemäß des Basler Übereinkommen in seiner aktuellen Fassung zu beachten. Chemikalien und weitere Materialien, welche im Falle von Freisetzung in die Umwelt eine Gefahr mit sich ziehen, sind in solcher Weise zu ermitteln bzw. zu handhaben, dass die Sicherheit bei Umgang mit diesen Stoffen (Beförderung, Lagerung, Nutzung, Recycling, Wiederverwendung oder Entsorgung) gewährleistet ist.



3. Compliance & ethisches Verhalten

3.1 Integrität / Anti-Korruption



Der Lieferant wirkt stets darauf hin, dass bei allen Geschäftsaktivitäten angemessene Integritätsstandards zugrunde gelegt werden. Der Lieferant duldet keine Art von Korruption, Bestechung oder Erpressung, noch beteiligt er sich daran. Verfahren zur Prävention, Überwachung und letztlich zu Durchsetzung der anwendbaren Normen sind zu implementieren, um die Einhaltung der entsprechenden Anti-Korruptions-Gesetzgebung zu gewährleisten.

3.2 Datenschutz/ Vertraulichkeit



Der Lieferant verwaltet und schützt alle bei ihm liegende personenbezogenen Daten in Übereinstimmung mit der geltenden Rechtsordnung, insb. der europäischen Datenschutzgrundverordnung (DSGVO). Des Weiteren achtet der Lieferant die Vertraulichkeit von Geschäftsinformationen anderer und schützt entsprechende Rechte. Rechte an geistigem Eigentum sind zu respektieren. Technologie- und Wissenstransfer haben so zu erfolgen, dass die geistigen Eigentumsrechte sowie Kunden-/Patienteninformationen stets geschützt sind.

3.3 Fairer Wettbewerb



Die Regeln für einen fairen Wettbewerb sind unabdingbare Voraussetzung für eine leistungsorientierte Marktwirtschaft, um wirtschaftliche Effizienz, Entwicklung und Innovationen zu fördern. Daher achtet und fördert der Lieferant den fairen Wettbewerb und agiert in Übereinstimmung mit allen geltenden Wettbewerbs- bzw. Kartellgesetzen.

III. Anforderungen an Lieferanten des Universitätsklinikum Frankfurt

Das Universitätsklinikum Frankfurt behält sich entsprechend § 6 Abs. 4 Nr. 4 LkSG vor, in begründeten Fällen beim Lieferanten angemessene risikobasierte Kontrollmaßnahmen hinsichtlich der Einhaltung aller anwendbaren Gesetze und Rechtsvorschriften, einschließlich dieses Code of Conduct für Lieferanten, durchzuführen. Gegenüber Lieferanten, welche die obenstehenden Anforderungen/ Sorgfaltspflichten/ Verbote nicht beachten, behält sich das Universitätsklinikum Frankfurt vor, geeignete Maßnahmen zu ergreifen, welche letztlich auch zu einem Aussetzen oder Beenden der Lieferbeziehung führen können.

IV. Kenntnisnahme und Einverständnis des Lieferanten

Ein Lieferant des Universitätsklinikum Frankfurt verpflichtet sich, mit der Annahme und Umsetzung des Vertrages, entsprechend der in diesem Dokument aufgeführten Aspekte, verantwortungsvoll zu handeln sowie die enthaltenen Anforderungen einzuhalten.





Dienstvertrag (Langfassung)

Vertrag über IT-Dienstleistungen

Inhaltsangabe



Dienstvertrag (Langfassung)

Vertrag über IT-Dienstleistungen

zwischen

Universitätsklinikum Frankfurt
Theodor-Stern-Kai 7
60590 Frankfurt am Main

Vertragsnummer/Kennung Auftraggeber: 20261019

„Auftraggeber“

und _____

Vertragsnummer/Kennung Auftragnehmer: _____

„Auftragnehmer“

wird folgender Vertrag geschlossen:

1 Gegenstand und Bestandteile des Vertrages

1.1 Vertragsgegenstand

Gegenstand des Vertrages sind Dienstleistungen des Auftragnehmers Gegenstand des Vertrages sind Managed-Services, die für die Übernahme, Fortführung, Steuerung und Weiterentwicklung der LAN- und WLAN-Infrastruktur des Auftraggebers erforderlich sind.

Der Auftragnehmer übernimmt die operative Verantwortung für die im Scope befindlichen Netzwerkkomponenten und Betriebsprozesse. Zum Leistungsgegenstand gehören insbesondere die Betriebsübernahme, der laufende Managed Service, Incident-, Problem-, Change-, Release- und Configuration-Management, Monitoring, Reporting, Dokumentation, Lifecycle-Management, Unterstützung bei EoL-/EoS-Risiken, Unterstützung bei RMA- und Herstellerprozessen sowie Integrationsleistungen für bereitgestellte oder separat beschaffte Komponenten. Die Lieferung der aktiven Netzwerkhardware ist nicht Gegenstand der regulären Leistung. Soweit Hardware, Lizenzen oder Herstellerwartung benötigt werden, erfolgt die Beschaffung grundsätzlich über den Auftraggeber oder über gesonderte Beschaffungswege. Der Auftragnehmer hat jedoch die Fähigkeit nachzuweisen, diese Komponenten technisch zu bewerten, in den Betrieb zu übernehmen und in die Serviceprozesse zu integrieren.

Die Leistung ist in mehrere Betriebs- und Projektphasen gegliedert: Service Ownership Transfer (SOT), Current Mode of Operation (CMO), Stabilisierung und Zielbildplanung, Integrations- und Modernisierungsphase, Future Mode of Operation (FMO) sowie eine Exit-Phase.

Die Leistungen sind insgesamt als Managed Service zu verstehen und nicht als einzelvorgangsbezogene Unterstützung ohne Gesamtverantwortung. Die Leistung muss die Anforderungen eines Klinikums mit KRITIS-Bezug berücksichtigen

Die Einzelheiten des Leistungsumfangs ergeben sich aus der beigefügten **Anlage L – Leistungsbeschreibung und Anforderungen „Managed-Services-LAN“**.

.

1.2 Vertragsbestandteile

Es gelten als Vertragsbestandteile:

1.2.1 dieser Vertragstext mit den folgenden Anlagen:

Dienstvertrag (Langfassung)

Anlage Nr.	Bezeichnung	Datum/Version	Anzahl Seiten
1	Anlage L - Leistungsbeschreibung		
2	Anlage P - Preismatrix		
3	AVV		
4	Code of Conduct (CoC) des Universitätsklinikums Frankfurt		
5	Anlagen und Unterlagen gemäß Abschnitt VI. A der Aufforderung zur Abgabe eines Angebots		

- ☒ Es gelten die Anlagen in folgender Rangfolge __1-5__. Die Anlagen stehen untereinander in der Reihenfolge ihrer Nummerierung; im Kollisionsfall geht die niedrigere Nummer der höheren Nummer vor).

1.2.2 die Ergänzenden Vertragsbedingungen für IT-Dienstleistungen (EVB-IT Dienstleistungs-AGB) in der bei Bereitstellung der Vergabeunterlagen geltenden Fassung einschließlich der Muster 1 und 2

1.2.3 sowie nachrangig die Allgemeinen Vertragsbedingungen für die Ausführung von Leistungen (VOL/B) in der bei Bereitstellung der Vergabeunterlagen geltenden Fassung.

Die EVB-IT Dienstleistungs-AGB stehen unter evb-it.gov.de zur Einsichtnahme bereit. Die VOL/B wurde im Bundesanzeiger AT Nr. 178a vom 23. September 2003 veröffentlicht.

Soweit Allgemeine Geschäftsbedingungen im Sinne von § 305 BGB in den hier referenzierten Dokumenten des Auftragnehmers bzw. den sonstigen vom Auftragnehmer beigefügten Anlagen zu diesem Vertrag Regelungen in den EVB-IT Dienstleistungs-AGB widersprechen, sind sie ausgeschlossen, soweit nicht eine anderweitige Vereinbarung in den EVB-IT Dienstleistungs-AGB zugelassen ist.

Weitere Geschäftsbedingungen sind ausgeschlossen, soweit in diesem Vertrag nichts anderes vereinbart ist.

Für alle in diesem Vertrag genannten Beträge gilt einheitlich der Euro als Währung. Die vereinbarten Vergütungen verstehen sich zuzüglich der gesetzlichen Umsatzsteuer, soweit Umsatzsteuerpflicht besteht.

Die mit * gekennzeichneten Begriffe sind am Ende der EVB-IT Dienstleistungs-AGB definiert.

2 Überblick über die vereinbarten Leistungen

Der Auftragnehmer erbringt für den Auftraggeber folgende Dienstleistungen:

- ☒ Beratung
- ☐ Projektleitungsunterstützung
- ☐ Schulung
- ☒ Einführungsunterstützung
- ☒ Betreiberleistungen
- ☐ Benutzerunterstützungsleistungen
- ☐ Providerleistungen ohne Inhaltsverantwortlichkeit
- ☒ Unterstützung bei Planungsleistungen
- ☐ Unterstützung bei Softwareentwicklung
- ☒ Hotline
- ☒ sonstige Dienstleistungen

3 Beschreibung der Leistungen/Laufzeit und Kündigung

3.1 Art, Umfang und Termine

Art, Umfang und Termine der zu erbringenden Leistungen ergeben sich aus der folgenden Tabelle (Termin- und Leistungsplan):

Dienstvertrag (Langfassung)

Lfd. Nr.	Leistung (ggf. Verweis auf Anlage)	Ort der Leistung	MVD ¹	Beginn ²	Ende/Termin ³
1	Service Ownership Transfer (SOT): Übernahmevorbereitung, Due Diligence, Tool- und Prozessanbindung Verbindliches Ergebnis: Abnahmefähige Betriebsübernahme	Universitätsklinikum Frankfurt.		Mit Zuschlagserteilung.	Mit Erfüllung der in Ziffer 22.1 der Anlage L –Leistungs- beschreibung zur Betriebsübernahme definierten Abnahmekriterien.
2	Current Mode of Operation (CMO): Betrieb der bestehenden Cisco-Infrastruktur; Verbindliches Ergebnis: Stabiler Managed Service für den Bestand	Universitätsklinikum Frankfurt.		Nach formaler SOT-Abnahme.	Bis vollständige Überführung der jeweiligen Netzbereiche in den FMO, längstens bis Vertragsende (Vertragsmonat 60)
3	Stabilisierung und Zielbildplanung: Bewertung des Bestands, Risikoanalyse, Zielbild und Integrationsplanung; Verbindliches Ergebnis: Freigegebenes Zielbild- und Umsetzungskonzept	Universitätsklinikum Frankfurt.		Nach formaler SOT-Abnahme.	Mit Konzeptabnahme gemäß Anlage L - Leistungsbeschreibung, Ziffer 22.1.
4	Integrations- und Modernisierungsphase: Integration bereitgestellter oder separat beschaffter Komponenten; Verbindliches Ergebnis: Überführung definierter Netzbereiche in den Zielbetrieb	Universitätsklinikum Frankfurt.		Mit Bereitstellung der ersten Komponenten durch den Auftraggeber.	Stufenweise mit Integrationsabnahmen und Betriebsabnahmen FMO je Netzbereich gemäß Anlage L, Ziffer 22.1; längstens bis Vertragsende (Vertragsmonat 60).
5	Future Mode of Operation (FMO): Betrieb modernisierter Netzbereiche mit höherem Standardisierungsgrad; Verbindliches Ergebnis: Messbarer Zielbetrieb	Universitätsklinikum Frankfurt.		Mit erster formaler Betriebsabnahme FMO eines Netzbereichs gemäß Anlage L, Ziffer 22.1; modellhaft ab Vertragsmonat 25 (FMO Phase A) gemäß Anlage P.	Vertragsende (Vertragsmonat 60).
6	Exit/Providerwechsel: Geordnete Übergabe, Datenexport, Wissenstransfer; Verbindliches Ergebnis: Übergabefähiger Service	Universitätsklinikum Frankfurt.		Spätestens sechs Monate vor Vertragsende.	Vertragsende (Vertragsmonat 60).
7	Herstellerbezogener Software-Support:	Universitätsklinikum Frankfurt/Remote.		Ab SOT-Abnahme (auf Abruf).	Bis Vertragsende (Vertragsmonat 60).

Dienstvertrag (Langfassung)

Lfd. Nr.	Leistung (ggf. Verweis auf Anlage)	Ort der Leistung	MVD ¹	Beginn ²	Ende/Termin ³
	Leistungen zur Prüfung, Koordination und optionalen Einbuchung eines herstellerbezogenen Software-Supports für im Scope befindliche Bestandskomponenten.				
8	Betriebsübernahme Sachsenhausen: Betriebsübernahme, laufender Managed Service CMO/FMO für den Standort Sachsenhausen.	Standort Sachsenhausen.		Ab Vertragsmonat 25.	Bis Vertragsende (Vertragsmonat 60).
9	Optionale Leistungen: Einmalige Installations-, Montage- und Einbindungsleistungen für bis zu 2.000 WLAN-Access-Points sowie optional eine Nachausleuchtung/WLAN-Survey können auf Abruf des Auftraggebers beauftragt werden.	Universitätsklinikum Frankfurt.		Auf Abruf des Auftraggebers während der Vertragslaufzeit.	Bis Vertragsende (Vertragsmonat 60).

Fußnote	Erläuterung
1	MVD = Mindestvertragsdauer
2	wenn keine Vorgabe für Beginn, dann Feld leer lassen
3	z. B. festes Datum ggf. mit Uhrzeit oder „nach 48 Monaten“ (wenn Vertrag unbefristet, dann Feld leer lassen)

3.1.1 Abgrenzung dienst- und werkvertraglicher Komponenten

Dieser Vertrag ist seinem Schwerpunkt nach ein Dienstvertrag im Sinne der §§ 611 ff. BGB. Die Abgrenzung zwischen laufenden Service-Leistungen dienstvertraglicher Natur und einmaligen Werkleistungen richtet sich nach der Anlage L – Leistungsbeschreibung in Verbindung mit der Preismatrix (Anlage P – Preismatrix).

Als werkvertraglicher Erfolg sind die folgenden Gegenstände gemäß Ziffer 22.1 der Anlage L – Leistungsbeschreibung geschuldet:

- Betriebsübernahme und SLA-Startfähigkeit
- Zielbild- und Umsetzungskonzept
- Übernahme eines Netzbereichs oder einer Komponente
- Überführung eines Bereichs in den Zielbetrieb
- Vollständige Übergabe m

Dienstvertrag (Langfassung)

Die Vergütung für laufende Service-Leistungen wird nach Ablauf des jeweiligen Abrechnungszeitraums gemäß der Anlage L – Leistungsbescheidung und der Anlage P – Preismatrix fällig. Die Vergütung für den Herstellerübergreifenden Software-Support und die Optionalen Leistungen erfolgt gemäß der Anlage P – Preismatrix gesondert nach tatsächlich beauftragtem und nachgewiesenem Herstellersupport sowie Abruf der optionalen Leistungen. Die Vergütung für einmalige Werkleistungen wird nach Abnahme gemäß den besonderen Abnahmebestimmungen in Anlage L – Leistungsbeschreibung fällig. Eine stillschweigende Abnahme durch Inbetriebnahme oder Nutzung ist ausgeschlossen.

3.1.2 Phasenstruktur und Parallelbetrieb CMO/FMO

Die Leistung gliedert sich in die in Anlage L – Leistungsbeschreibung, Kapitel 2, definierten Betriebsphasen. Die Phasen bilden die verbindliche Grundlage für Aufgaben, Verantwortlichkeiten, Abnahmen, SLA-Wirksamkeit und Vergütung. SLA-Verpflichtungen gelten erst ab dem Zeitpunkt der formalen SOT-Abnahme gemäß Anlage L – Leistungsbeschreibung, Kapitel 22.

Während der Vertragslaufzeit können CMO- und FMO-Bereiche parallel bestehen. Der Auftragnehmer muss beide Betriebszustände beherrschen und sauber voneinander abgrenzen. Die Zuordnungslogik, Dokumentationspflichten und Abrechnungsregeln für den Parallelbetrieb richten sich nach Anlage L – Leistungsbeschreibung, Kapitel 16.4 und 20.4 bis 20.7. Eine doppelte Abrechnung desselben Ports als CMO und FMO ist ausgeschlossen.

Die Leistung gemäß Nummer 3.1 lfd. Nr. 7 (Herstellerbezogener Software-Support) stellt keine eigenständige Betriebsphase im Sinne der vorstehenden Phasenstruktur dar; sie ist eine phasenübergreifende, auf Abruf zu erbringende Leistung, die – soweit ein herstellenseitiger Software-Support für die jeweilige Bestandskomponente verfügbar und durch den Auftraggeber freigegeben ist – während der gesamten Vertragslaufzeit parallel zu den übrigen Betriebsphasen gilt und im Einzelnen den Regelungen gemäß Anlage L – Leistungsbeschreibung, Kapitel 17.6, unterliegt.

Der Managed Service muss so ausgestaltet sein, dass zusätzliche Standorte, Gebäude, Funktionsbereiche oder organisatorisch zugeordnete Einheiten des Auftraggebers in den Scope aufgenommen werden können. Dies gilt insbesondere für Netzbereiche, die während des Verfahrens oder während der Vertragslaufzeit zusätzlich in den Verantwortungsbereich des Auftraggebers fallen. Der Bestand Sachsenhausen ist als gesonderter, zeitversetzt einzubeziehender Scope auszuweisen. Er wird nicht Bestandteil des initialen CMO-Betriebs des UKF-Campus Frankfurt, sondern planmäßig nach Ablauf von 24 Monaten ab Leistungsbeginn in den Managed Service überführt. Die laufende Servicevergütung, SLA-Wirksamkeit und Mengenberücksichtigung für Sachsenhausen beginnen erst mit der formalen Aufnahme in den Leistungsumfang. Die Abbildung erfolgt in der Preismatrix über einen separaten Mengen- und Wertungsansatz für Sachsenhausen ab Monat 25.

Die in der Tabelle 3.1 aufgelisteten Leistungsbestandteile sind nicht abschließend. Im Übrigen wird auf die Regelungen in Anlage L – Leistungsbeschreibung und Anlage P – Preismatrix verwiesen.

- ☒ Feiertage im Sinne dieses Vertrages sind die Feiertage im **Bundesland Hessen** (siehe Ziffer 5.1 EVB-IT Dienstleistungs-AGB).

3.2 Einmalig zu erbringende Leistungen

- ☒ Die Leistungen gemäß Nummer 3.1 lfd. Nr. **1, 3, 4, 6** werden einmalig erbracht.

3.3 Regelmäßig zu erbringende Leistungen

- ☒ Die Leistungen gemäß Nummer 3.1 lfd. Nr. **2, 5, 8** werden
 - ☐ in folgendem Zyklus erbracht:
 - ☐ wöchentlich
 - ☐ monatlich
 - jeweils
 - ☐ an folgenden Tagen: _____ (Wochentag(e) bzw. bei monatlichen Zyklen auch „1. Montag im Monat“)
 - ☐ in der Zeit von _____ bis _____ (Uhrzeit)
 - nicht jedoch an Feiertagen.



Dienstvertrag (Langfassung)

- ☒ in folgenden Zyklen zu folgenden Zeiten erbracht: gem. **Anlage L – Leistungsbeschreibung und Anlage P – Preismatrix**.

3.4 Leistungen, die nur auf Abruf erbracht werden sollen

- ☒ Die Leistungen gemäß Nummer 3.1 lfd. Nr. **7, 9** werden nur auf Abruf erbracht.
- ☐ Der Mindestvorlauf für den Abruf beträgt _____ (Stunden/Tage).
- ☐ Die geschätzte Abnahme beträgt _____ (Stunden/Tage) pro _____ (z. B. Vertragsmonat/Vertragsquartal/Vertragsjahr/Vertragslaufzeit).
- ☐ Die vereinbarte Mindestabnahme beträgt _____ (Stunden/Tage) pro _____ (z. B. Vertragsmonat, Vertragsquartal, Vertragsjahr, Vertragslaufzeit).
- ☐ Die Mindestabnahme für Leistungen, die Reisen erforderlich machen, beträgt pro Abruf _____ (Stunden/Tage).

Soweit Leistungen nur auf Abruf zu erbringen sind, hält sich der Auftragnehmer in dem vorgenannten Zeitraum zur Leistungserbringung bereit.

3.5 Abweichende Kündigungsregelung

- ☐ Abweichend von Ziffer 15.1 EVB-IT Dienstleistungs-AGB beträgt die Kündigungsfrist _____ Monat(e) zum Ablauf eines _____ (z.B. Kalendermonats/Kalendervierteljahres/Kalenderjahres).
- ☐ Abweichend von Ziffer 15.1 EVB-IT Dienstleistungs-AGB wird bei vereinbarter fester Laufzeit ein Sonderkündigungsrecht gem. Anlage Nr. _____ vereinbart.

4 Vergütung

4.1 Vergütung nach Aufwand

- ☐ Die Leistungen gemäß
- ☐ Nummer 3.1 lfd. Nr. _____ werden nach Aufwand gemäß Kategorie(n) _____ aus Nummer 4.1.1
- ☐ mit einer Obergrenze in Höhe von _____ Euro
- ☐ Nummer 3.1 lfd. Nr. _____ werden nach Aufwand gemäß Kategorie(n) _____ aus Nummer 4.1.1
- ☐ mit einer Obergrenze in Höhe von _____ Euro
- ☐ Nummer 3.1 lfd. Nr. _____ werden nach Aufwand gemäß Kategorie(n) _____ aus Nummer 4.1.1
- ☐ mit einer Obergrenze in Höhe von _____ Euro

vergütet.

4.1.1 Kategorien

Lfd. Nr.	Bezeichnung der Kategorie	Stundensatz für Tätigkeiten innerhalb der zuschlagsfreien Zeiten	Tagessatz für Tätigkeiten innerhalb der zuschlagsfreien Zeiten	Zuschläge in Prozent auf die Stunden- und Tagessätze Montag bis Freitag (Arbeitstage) außerhalb der zuschlagsfreien Zeiten	Zuschläge in Prozent auf die Stunden- und Tagessätze Samstag von _____ bis _____	Zuschläge in Prozent auf die Stunden- und Tagessätze Samstag von _____ bis _____	Zuschläge in Prozent auf die Stunden- und Tagessätze Sonn- und Feiertage von _____ bis _____	Zuschläge in Prozent auf die Stunden- und Tagessätze Sonn- und Feiertage von _____ bis _____
				_____ %	_____ %	_____ %	_____ %	_____ %

Festlegung der zuschlagsfreien Zeiten:

Dienstvertrag (Langfassung)

Arbeitstag	zuschlagsfreie Zeiten
Montag bis Donnerstag	von ____ bis ____ Uhr
Freitag	von ____ bis ____ Uhr

- ☐ Weitere Vereinbarungen gemäß Anlage Nr. ____.

4.1.2 Abweichende Regelungen für die Bestimmung und Vergütung von Personentagesätzen

- ☐ Abweichend von Ziffer 9.2.4 Satz 2 EVB-IT Dienstleistungs-AGB können bei entsprechendem Nachweis pro Kalendertag bis zu 10 Stunden abgerechnet werden.
- ☐ Abweichend von Ziffer 9.2.4 Sätze 2 und 3 Dienstleistungs-AGB kann ein voller Tagessatz nur in Rechnung gestellt werden, wenn mindestens 10 Stunden geleistet wurden. Werden weniger als 10 Zeitstunden pro Tag geleistet, sind diese anteilig in Rechnung zu stellen.
- ☐ weitere Vereinbarungen gemäß Anlage Nr. ____.

4.1.3 Reisekosten/Nebenkosten*/Materialkosten/Reisezeiten

- ☐ Reisekosten werden nicht gesondert vergütet.
- ☐ Reisekosten werden vergütet gemäß Anlage Nr. ____.
- ☐ Nebenkosten* werden nicht gesondert vergütet.
- ☐ Nebenkosten* werden vergütet gemäß Anlage Nr. ____.
- ☐ Materialkosten werden nicht gesondert vergütet.
- ☐ Materialkosten werden vergütet gemäß Anlage Nr. ____.
- ☐ Reisezeiten werden nicht gesondert vergütet.
- ☐ Reisezeiten werden zu 50 % als Arbeitszeiten vergütet.
- ☐ Reisezeiten werden vergütet gemäß Anlage Nr. ____.

4.1.4 Preisanpassung

- ☐ Es wird eine Preisanpassung
- ☐ gemäß Ziffer 9.5 EVB-IT Dienstleistungs-AGB
- ☐ gemäß Anlage Nr. ____
- für die Kategorien gemäß Nummer 4.1.1 vereinbart.

4.1.5 Fälligkeit und Zahlung

Die Vergütung ist abweichend von Ziffer 9.3 EVB-IT Dienstleistungs-AGB nicht monatlich nachträglich fällig, sondern

- ☐ zum 15. des auf die Leistungserbringung folgenden Monats.
- ☐ wie folgt ____.
- ☐ gemäß Anlage Nr. ____.

4.1.6 Besondere Bestimmungen zur Vergütung nach Aufwand

- ☐ Besondere Bestimmungen zur Vergütung nach Aufwand sind in Anlage Nr. ____ vereinbart.

Dienstvertrag (Langfassung)

4.2 Vergütung zum Pauschalpreis

☒ Die Leistungen gemäß Nummer 3.1 lfd. **Nr. 1 bis 9** werden zum Pauschalpreis **gem. Anlage P – Preisblatt**. Euro vergütet.

☐ Es werden folgende Abschlagszahlungen vereinbart:

Betrag: _____ Anlass: _____,

Betrag: _____ Anlass: _____,

Betrag: _____ Anlass: _____.

4.3 Rechnungsadresse

Rechnungen sind an folgende Anschrift zu richten:

Universitätsklinikum Frankfurt

Zentraler Rechnungseingang

invoice@ukffm.de

5 Service- und Reaktionszeiten*

☐ Für die Leistungen gemäß Nummer 3.1 lfd. _____ werden folgende Service- und Reaktionszeiten* vereinbart:

5.1 Servicezeiten*

Tag	Uhrzeit
_____ bis _____	von _____ bis _____ Uhr
An Sonntagen	von _____ bis _____ Uhr
An Feiertagen	von _____ bis _____ Uhr

☒ Weitere Vereinbarungen zu Servicezeiten* gemäß Anlage **L – Leistungsbeschreibung**.

5.2 Reaktionszeiten*

Leistung gemäß Nummer 3.1	Anlass/Problemkategorie	Reaktionszeit* in Stunden

☒ Die Reaktionszeiten* werden in Anlage **L – Leistungsbeschreibung** festgelegt.

Reaktionszeiten* beginnen ausschließlich mit Zugang der entsprechenden Meldung oder dem Eintritt des vereinbarten Ereignisses während der vereinbarten Servicezeiten* und laufen ausschließlich während der vereinbarten Servicezeiten*.

Ergänzend können in Nummer 12 für die Nichteinhaltung der o.g. Zeiten Vertragsstrafen vereinbart werden.

6 Ansprechpartner

Ansprechpartner des Auftraggebers (Name, Adresse, Abteilung, Telefon, Fax, E-Mail):

Ansprechpartner des Auftragnehmers (Name, Adresse, Abteilung, Telefon, Fax, E-Mail):

Dienstvertrag (Langfassung)

7 Besondere Anforderungen an Mitarbeiter des Auftragnehmers

- ☐ Mindestanforderungen an das einzusetzende Personal des Auftragnehmers:

Lfd. Nr.	Position	Schlüsselposition gemäß Ziffer 8.3 EVB-IT Dienstleistungs-AGB (ja/nein)	Fachliche Qualifikation	Sicherheitsüberprüfung Ü 1, 2 oder 3 ¹	Sonstige Anforderungen, z. B. weitere Sicherheitsanforderungen

¹ Stufen der Sicherheitsüberprüfung gemäß Sicherheitsüberprüfungsgesetz

- ☐ Abweichend von Ziffer 8.1 EVB-IT Dienstleistungs-AGB ist der Auftragnehmer verpflichtet, für die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ nur Personal einzusetzen, welches bereit ist, sich aufgrund des Verpflichtungsgesetzes verpflichten zu lassen.
- ☐ Abweichend von Ziffer 8.1 EVB-IT Dienstleistungs-AGB ist der Auftragnehmer berechtigt, für die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ auch Personal einzusetzen, welches lediglich in folgender Sprache zu kommunizieren in der Lage ist: _____.
- ☒ Mindestanforderungen an das einzusetzende Personal des Auftragnehmers ergeben sich aus Anlage Nr. **L – Leistungsbeschreibung**.

8 Mitwirkungsleistungen des Auftraggebers

- ☐ Folgende Mitwirkungsleistungen des Auftraggebers werden abweichend und zusätzlich zu Ziffer 14 EVB-IT Dienstleistungs-AGB vereinbart: _____.
- ☒ Die Mitwirkungsleistungen des Auftraggebers ergeben sich abweichend und zusätzlich zu Ziffer 14 EVB-IT Dienstleistungs-AGB aus **L – Leistungsbeschreibung**.

9 Abweichende Nutzungsrechte an den Leistungsergebnissen, Erfindungen

Für folgende Leistungsergebnisse werden von Ziffer 3.1 EVB-IT Dienstleistungs-AGB abweichende Nutzungsrechte vereinbart:

- ☐ Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. _____ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass statt des dort aufgeführten nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt wird, vorbestehende Werke jedoch ausgenommen.
- ☐ Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. _____ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass statt des dort aufgeführten nicht ausschließlichen Nutzungsrechts ein ausschließliches Nutzungsrecht gewährt wird, vorbestehende Werke jedoch ausgenommen: _____.
- ☐ Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. _____ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass eine gewerbliche Verbreitung uneingeschränkt möglich ist.
- ☐ Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. _____ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass eine gewerbliche Verbreitung uneingeschränkt möglich ist, _____.
- ☐ Für alle Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. _____ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass jegliche gewerbliche Verbreitung ausgeschlossen ist.
- ☐ Für folgende Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. _____ gilt Ziffer 3.1 EVB-IT Dienstleistungs-AGB mit der Maßgabe, dass jegliche gewerbliche Verbreitung ausgeschlossen ist: _____.
- ☐ Für alle Ergebnisse der Leistungen (z.B. Dokumentationen) gemäß Nummer 3.1 lfd. Nr. _____ gilt abweichend von Ziffer 3.1 EVB-IT Dienstleistungs-AGB folgende von openCode* freigegebene Lizenz: _____.



Dienstvertrag (Langfassung)

- ☐ **Bereitstellung als Open Source Software***: Die Bereitstellung der Ergebnisse der Leistungen gemäß Nummer 3.1 lfd. Nr. _____ erfolgt als Open Source Software* (ergänzend zur Rechteeinräumung gemäß Ziffer 3.1 EVB-IT Dienstleistungs-AGB und zu ggf. vorstehend vereinbarten Änderungen daran).
- Zusätzlich bzw. abweichend davon gilt folgendes. Die Bereitstellung der Software
- ☐ muss wie vorstehend beschrieben, jedoch unter **von openCode* freigegebenen Lizenzen** erfolgen.
 - ☐ muss wie vorstehend beschrieben, jedoch unter von openCode* freigegebenen Lizenzen, **die keinen Copyleft*-Effekt** haben, erfolgen (sog. permissive Lizenzen, z.B. MIT- oder Apachelizenz > Version 1.0).
 - ☐ muss wie vorstehend beschrieben, jedoch unter von openCode* freigegebenen Lizenzen **mit Copyleft*-Effekt** zur Verfügung gestellt werden (sog. reziproke Lizenzen, z.B. GNU GPL oder LGPL).
 - ☐ muss wie vorstehend beschrieben, jedoch unter der/den **folgenden Lizenz(en)** zur Verfügung gestellt werden, die den Anforderungen an **Open Source Software*** entsprechen: _____.
 - ☐ Soweit die Ergebnisse der Leistungen als **Open Source Software*** bereitgestellt werden müssen, wird vereinbart, dass diese ggf. gemeinsam mit folgender Software genutzt und verbreitet wird (siehe Ziffer 3.2 EVB-IT Dienstleistungs-AGB): _____.
- ☐ Von Ziffer 3.1 EVB-IT Dienstleistungs-AGB abweichende Nutzungsrechte sind in Anlage Nr. _____ geregelt.
- ☐ Für Erfindungen, die anlässlich der Vertragserfüllung gemacht werden, gelten abweichend von Ziffer 4 EVB-IT Dienstleistungs-AGB die Regelungen in Anlage Nr. _____.
- ☐ Abweichend von Ziffer 3.4 EVB-IT Dienstleistungs-AGB darf der Auftragnehmer **vorbestehende Software bzw. Softwareteile** auch ohne Zustimmung des Auftraggebers in die Leistungsergebnisse integrieren, sofern daran Nutzungsrechte wie an den Leistungsergebnissen im Übrigen verschafft werden.

10 Quellcode* und Software Bill of Materials (SBOM)

Im Falle der Erstellung oder Bearbeitung von Software:

- ☐ ist gemäß Ziffer 3.7 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes* auf folgendem vom Auftraggeber zur Verfügung gestellten Quellcoderepository zu speichern: _____.
- ☐ wird abweichend von Ziffer 3.7 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes* wie folgt gespeichert und dem Auftraggeber zur Verfügung gestellt: _____.
- ☐ wird abweichend von Ziffer 3.7 EVB-IT Dienstleistungs-AGB der jeweils aktuelle Stand der Software, einschließlich der Quellcodes* nicht täglich sondern _____ (z.B. am Ende jeder Arbeitswoche) abgespeichert.
- ☐ erfolgt die Übergabe des Quellcodes* auch am Ende jedes Leistungsmonats in elektronischer Form auf einem Datenträger.

Die Pflichten in Bezug auf die Übergabe des Quellcodes* von Open Source Software* bleiben von den vereinbarten Abweichungen nach dieser Nummer 10 unberührt.

- ☐ Der Auftragnehmer stellt dem Auftraggeber eine Software Bill of Materials (SBOM) gemäß BSI TR-03183-2 für den jeweils aktuellen Stand der Software
 - ☐ im Format SPDX
 - ☐ im Format CycloneDX

zur Verfügung.

11 Abweichende Haftungsregelungen

- ☐ Abweichend von Ziffer 13.1 EVB-IT Dienstleistungs-AGB beträgt die Haftungsobergrenze bei leicht fahrlässigen Pflichtverletzungen
 - ☐ pro Schadensfall _____ Euro.
 - ☐ insgesamt für diesen Vertrag _____ Euro.
- ☐ Abweichend von Ziffer 13.1 EVB-IT Dienstleistungs-AGB gelten für die Haftung bei leicht fahrlässigen Pflichtverletzungen die Regelungen gemäß Anlage Nr. _____.
- ☒ Abweichend von Ziffer 13.3 EVB-IT Dienstleistungs-AGB haftet der Auftragnehmer auch für entgangenen Gewinn.



Dienstvertrag (Langfassung)

- ☒ Haftungsregelung bei EoL-/EoS-Komponenten: In Abweichung von Kapitel 17.5 der Anlage L verzichtet der Auftraggeber auf Haftungsansprüche für Schäden, die nachweislich und kausal durch den gewünschten Weiterbetrieb von Systemen oder Komponenten nach Erreichen des End-of-Life (EoL) bzw. End-of-Support (EoS) entstehen. Im Übrigen bleibt das Verbot der pauschalen Entlastung des Auftragnehmers gemäß Kapitel 17.5 der Anlage L vollumfänglich bestehen.

12 Vertragsstrafen

- ☐ Als vertragsstrafenrelevant im Sinne von Ziffer 10.3 EVB-IT Dienstleistungs-AGB gelten die in Nummer 3.1 lfd. Nr. _____ vereinbarten Leistungstermine.
- ☐ Abweichend von Ziffer 10.3 EVB-IT Dienstleistungs-AGB wird für Leistungen gemäß Nummer 3.1 lfd. Nr. _____ die Vertragsstrafenregelung gemäß Anlage Nr. _____ vereinbart.
- ☐ Für die Nichteinhaltung von Reaktionszeiten* gilt die Vertragsstrafenregelung aus Ziffer 10.4 EVB-IT Dienstleistungs-AGB.
- ☐ Für die Nichteinhaltung von Reaktionszeiten* gelten die Regelungen in Anlage Nr. _____.
- ☐ Für jeden Verstoß gegen Ziffer 1.5 oder Ziffer 1.6 der EVB-IT Dienstleistungs-AGB wird eine Vertragsstrafe in Höhe von _____ Euro vereinbart. Dies gilt nicht, wenn der Auftragnehmer den Verstoß nicht zu vertreten hat.
- ☐ Für jeden Verstoß des Auftragnehmers gegen die Regelung im ersten Aufzählungspunkt der Ziffer 8.3 EVB-IT Dienstleistungs-AGB wird eine Vertragsstrafe in Höhe von _____ Euro vereinbart. Dies gilt nicht, wenn der Auftragnehmer den Verstoß nicht zu vertreten hat.

13 Weitere Regelungen

13.1 Datenschutz, Geheimhaltung und Sicherheit

Der Auftragnehmer verpflichtet sich für die Laufzeit des Vertrages

- ☒ bei der Erbringung der vertraglichen Leistungen die Regelungen zur IT-Sicherheit gemäß Anlage L – **Leistungsbeschreibung** zu beachten.
- ☐ der Geheimschutzbetreuung gemäß Anlage Nr. _____ zu unterstellen.
- ☒ die Regelungen des Auftraggebers zur Sicherheit am Einsatzort gemäß Anlage L – **Leistungsbeschreibung** zu beachten.
- ☒ folgende weitere Regelungen einzuhalten: **NIS2-Richtlinie, BSI-Gesetz (BSIG)**.
- ☒ Ergänzend zu bzw. abweichend von Ziffer 19 EVB-IT Dienstleistungs-AGB ergeben sich Regelungen zur Geheimhaltung bzw. zur Sicherheit aus Anlage L – **Leistungsbeschreibung**.
- ☐ Da durch den Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden sollen (Auftragsverarbeitung), treffen die Parteien in Anlage Nr. __3__ eine schriftliche Vereinbarung, die zumindest die gesetzlichen Mindestanforderungen beinhaltet.
- ☒ Die Parteien treffen sonstige Vereinbarungen zum Datenschutz gemäß Anlage Nr. L – **Leistungsbeschreibung**.

13.2 Haftpflichtversicherung

- ☒ Der Nachweis einer Haftpflichtversicherung gemäß Ziffer 18 EVB-IT Dienstleistungs-AGB wird vereinbart.

13.3 Teleservice*

- ☐ Soweit der Auftragnehmer zur Leistung durch Teleservice* berechtigt ist, wird er diesen ausschließlich aufgrund der Teleservicevereinbarung gemäß Anlage Nr. _____ erbringen und darf dabei ausschließlich folgendes automatisiertes Verfahren einsetzen: _____ (Produktbezeichnung). Dieses Verfahren muss neben den Anforderungen aus Ziffer 1.5 EVB-IT Dienstleistungs-AGB auch den Anforderungen aus der Anlage Nr. _____ genügen.

13.4 Dokumentations- und Berichtspflichten

- ☐ Abweichend von Ziffer 6 EVB-IT Dienstleistungs-AGB dokumentiert der Auftragnehmer die Leistungen gemäß Nummer 3.1 lfd. Nr. _____ nicht in deutscher, sondern in _____ Sprache.
- ☒ Weitere Dokumentations- und Berichtspflichten des Auftragnehmers ergeben sich aus Anlage Nr. L – **Leistungsbeschreibung**.



Dienstvertrag (Langfassung)

13.5 Interessenkonflikt

- ☐ Regelungen zur Vermeidung eines Interessenskonfliktes ergeben sich aus Anlage Nr. _____.

14 Pflichten nach Vertragsende

- ☒ Ergänzend zu Ziffer 16 EVB-IT Dienstleistungs-AGB ergeben sich weitere Vereinbarungen zu den Pflichten des Auftragnehmers nach Vertragsende aus Anlage Nr. Anlage L.

15 Sonstige Vereinbarungen

- ☒ Sonstige Vereinbarungen:

15.1 Service Level, Eskalation und Qualitätssicherung

Es gelten die in Anlage L – Leistungsbeschreibung in Ziffer 18 geregelten Service Level, Eskalation und Qualitätssicherungsregeln.

15.4 Personalwechsel

Der Auftragnehmer verpflichtet sich, nach jeder angemessenen und zumutbaren Möglichkeit dafür Sorge zu tragen, dass während der Laufzeit dieses EVB-IT Dienstvertrages die auf Seiten des Auftragnehmers zu Beginn dieses EVB-IT Dienstvertrages eingesetzten Mitarbeitenden bzw. Dritten (Subunternehmer, Erfüllungsgehilfen) nur bei unbedingt bestehender Notwendigkeit ersetzt werden. Der Wechsel von vom Auftragnehmer eingesetzten Dritten (Subunternehmern, Erfüllungsgehilfen) bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers, die dieser allerdings aus sachlichen Gründen verweigern darf. Dem Auftraggeber steht bei als Austausch vom Auftragnehmer vorgesehenen Mitarbeitenden bzw. Dritten (Subunternehmern, Erfüllungsgehilfen) hinsichtlich deren Auswahl sowie fachlicher Geeignetheit und Qualifikation ein Mitspracherecht zu. Der Auftragnehmer stellt für die gesamte Laufzeit dieses EVB-IT Dienstvertrages sicher, dass die auf Seiten des Auftragnehmers eingesetzten Mitarbeitenden bzw. Dritten (Subunternehmer, Erfüllungsgehilfen) über die für die vertragsgemäße Durchführung dieses EVB-IT Dienstvertrages erforderlichen Fachkenntnisse und Qualifikationen verfügen.

15.3 Änderungen und Ergänzungen

Änderungen und Ergänzungen dieses Vertrags bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Änderung des Schriftformerfordernisses.

15.4 Abtretung

Ohne vorherige schriftliche Zustimmung der anderen Partei ist keine Partei berechtigt, Rechte aus diesem Vertrag an Dritte abzutreten oder Verpflichtungen aus diesem Vertrag auf Dritte zu übertragen. Hiervon ist das Recht des Auftragnehmers nicht berührt, zur Durchführung des Auftrags Dritte mit der Erbringung von Leistungen zu beauftragen. Eine Rechtsbeziehung zwischen dem Auftraggeber und diesen Dritten wird hierdurch nicht geschaffen.

15.5 Sonstige Regelungen

(1) Mündliche Nebenabreden zu diesem Vertrag bestehen nicht.

(2) Vertrags- und Geschäftssprache ist Deutsch.

(3) Sollten einzelne Regelungen dieses Vertrages unwirksam oder undurchführbar sein oder werden, so bleibt hiervon die Wirksamkeit der anderen Vertragsbestimmungen unberührt. In diesem Fall ist die unwirksame oder undurchführbare Bestimmung durch eine gesetzlich zulässige, dem mit der unwirksamen oder undurchführbaren Regelung verfolgten wirtschaftlichen Zweck möglichst nahekommen-de Bestimmung zu ersetzen.

- ☐ Die sonstigen Vereinbarungen ergeben sich aus Anlage Nr. _____.

Unterschrift Auftraggeber

Unterschrift Auftragnehmer



Dienstvertrag (Langfassung)

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Datum, Name

Datum, Name

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen dem

Universitätsklinikum Frankfurt (Anstalt des öffentlichen Rechts),

vertreten durch den Vorstand

Theodor - Stern - Kai 7

60590 Frankfurt am Main

Ausführende Stellen, Verantwortliche nach Art. 4 DS-GVO

- Verantwortliche - nachstehend Auftraggeber genannt -

und dem/der

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Präambel

Die Parteien sind sich über die Bedeutung des Schutzes des Persönlichkeitsrechts beim Umgang mit personenbezogenen Daten bewusst und ihnen sind die dazu bestehenden rechtlichen, insbesondere datenschutzrechtlichen Vorschriften bekannt. Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien, die sich aus bestehenden oder künftigen Verträgen über Lieferungen und Leistungen ergeben, soweit diese eine Verarbeitung von personenbezogenen Daten des Auftraggebers oder seiner Patienten, insbesondere im Sinne der Datenschutzgrundverordnung (DS-GVO), durch den Auftragnehmer zum Gegenstand haben.

Inhalt

Präambel	2
1. Gegenstand und Dauer des Auftrags	3
2. Konkretisierung des Auftragsinhalts	3
3. Technisch-organisatorische Maßnahmen	4
4. Berichtigung, Einschränkung und Löschung von Daten	4
5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers	5
6. Unterauftragsverhältnisse	6
7. Kontrollrechte des Auftraggebers	7
8. Mitteilung bei Verstößen des Auftragnehmers	7
9. Weisungsbefugnis des Auftraggebers	8
10. Löschung und Rückgabe von personenbezogenen Daten	8
11. Informationspflichten, Schriftformklausel	8
12. Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB)	9
13. Haftung	10
14. Salvatorische Klausel	10
15. Rechtswahl, Gerichtsstand	10
Anlage 1 – Technisch-organisatorische Maßnahmen nach Art. 25	Fehler! Textmarke nicht definiert.
Anlage 2 – Kontaktdaten des Auftragnehmers	14
1. Datenschutzbeauftragte(r)	14
2. Ansprechpartner (wenn kein(e) Datenschutzbeauftragte(r) erforderlich ist)	14
3. ständiger Vertreter gemäß Art. 27 DS-GVO	14
Anlage 3 – Liste der Unterauftragnehmer des Auftragnehmers	15
Anlage 4 – Weisungsberechtigte Personen	16
1. beim Auftraggeber	16
2. beim Auftragnehmer	16

1. Gegenstand und Dauer des Auftrags

- (1) Gegenstand
- Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:für das Universitätsklinikum Frankfurt
- (2) Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist gemäß Hauptbeauftragung gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

- Auftragsinhalt ist die Durchführung von: für das Universitätsklinikum Frankfurt.
- (1) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

- ☐ Patientendaten / Personenstammdaten
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Adressdaten
- ☐ Gesundheitsdaten
- ☐ Vertragsabrechnungs- und Zahlungsdaten
- ☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Interessenten
- ☐ Besucher
- ☐ Bewerber
- ☐ Planungs- und Steuerungsdaten
- ☐ Auskunftsangaben
(von Dritten, z.B. Auskunftfeien, oder aus öffentlichen Verzeichnissen)
- ☐

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☐ Patienten
- ☐ Spender
- ☐ Interessenten
- ☐ Beschäftigte
- ☐ Lieferanten
- ☐ Handelsvertreter
- ☐ Ansprechpartner
- ☐ Abonnenten
- ☐

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung, sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen [**Anlage 1**].

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer

wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer unterstützt angesichts der Art der Verarbeitung den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DS-GVO genannten Rechte der betroffenen Person nachzukommen.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) ☐ Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.
- ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
- ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer bestellt: **[Anlage 2]**. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
- ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- b) ☐ oder: Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird benannt: **[Anlage 2]**.
- c) ☐ oder: Da der Auftragnehmer seinen Sitz außerhalb der Union hat, benennt er folgenden Vertreter nach Art. 27 Abs. 1 DS-GVO in der Union: **[Anlage 2]**.
- d) ☒ Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- e) ☒ Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen ist gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO **[Anlage 1]** sicherzustellen.
- f) ☒ Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- g) ☒ Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits-

- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- h) ☒ Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
- i) ☒ Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse, sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- j) ☒ Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) wie folgt beauftragen:

- ☐ Eine Unterbeauftragung ist unzulässig
- ☐ nach vorheriger ausdrücklicher schriftlicher Zustimmung des Auftraggebers
- ☐ Der Auftraggeber stimmt der Beauftragung der Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO.
[Anlage 3]

(3) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht innerhalb einer Frist von 14 Tagen, gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(4) Die Weitergabe von personenbezogenen Daten des Auftragnehmers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Eine weitere Auslagerung durch den Unterauftragnehmer

- ☐ ist nicht gestattet;
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
- ☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch (optional durch Auftragnehmer zu belegen):

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer wird Daten des Auftraggebers nur zur Erfüllung der vertraglich vereinbarten Leistungen und nach Weisung des Auftraggebers verarbeiten. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird. Weisungsberechtigte Personen des Auftraggebers sind in der **[Anlage 4]** benannt und sind mit den weisungsberechtigten Personen des Auftragnehmers zu vervollständigen.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Informationspflichten, Schriftformklausel

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Es gelten ausschließlich diese Bedingungen; Nebenabreden, Änderungen oder Ergänzungen dieser Bedingungen bedürfen für Ihre Wirksamkeit der Schriftform. Dieses gilt auch für die Abbedingung der Schriftformklausel.

12. Verpflichtung zur Geheimhaltung von Berufsgeheimnissen (§ 203 StGB)

(1) Im Rahmen dieses Auftrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.

Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich Personen, die an der beruflichen Tätigkeit eines Berufsgeheimnisträgers mitwirken und unbefugt ein fremdes Geheimnis offenbaren, das ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt geworden ist, strafbar machen nach § 203 Abs. 4 S. 1 StGB.

Zudem macht sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z.B. Subunternehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Auftraggeber weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde

(3) Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u.U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegt (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

(4) Der Auftragnehmer wird darauf hingewiesen, dass die sich in seinem Gewahrsam befindenden Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 Abs. 2 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

13. Haftung

Die Haftung richtet sich nach den allgemeinen Gesetzen insbesondere nach Artikel 82 DS-GVO.

14. Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages ganz oder teilweise unwirksam oder unanwendbar sein oder werden, oder sollte sich in dem Vertrag eine Lücke befinden, so soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen oder unanwendbaren Bestimmung oder zur Ausfüllung der Lücke soll eine angemessene Regelung treten, die, soweit rechtlich möglich, dem am nächsten kommt, was die Vertragsparteien gewollt haben oder nach dem Sinn und Zweck dieses Vertrages gewollt haben würden, wenn sie den Punkt bedacht hätten.

15. Rechtswahl, Gerichtsstand

Für etwaige Streitigkeiten aus den Verträgen oder damit im Zusammenhang stehenden Rechtsbeziehungen wird Frankfurt als Gerichtsstand vereinbart.

Für den Auftraggeber:

Name, Funktion:

Ort, Datum, Unterschrift:

Für den Auftragnehmer:

Name, Funktion: (*mindestens ppa.*)

Ort, Datum, Unterschrift:

Universitätsklinikum Frankfurt

Anlage 1 – Technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

Diese Anlage ergänzt den Vertrag zwischen dem Auftraggeber und dem Auftragnehmer. Ziel dieser Anlage ist die Festlegung und Einhaltung technischer und organisatorischer Maßnahmen (TOMs) nach dem aktuellen Stand der Technik, zum Schutz personenbezogener Daten und insbesondere zum Schutz besonders schutzwürdiger personenbezogener Daten, gemäß den geltenden Datenschutzgesetzen. Es handelt sich hierbei um Mindestanforderungen, die in jedem Fall mindestens vorliegen müssen. Technische- und organisatorische Maßnahmen die über die hier genannten hinausgehen bzw. im Rahmen der angegebenen Services näher spezifiziert werden sind beizufügen. Erweiterungen der Maßnahmen die dem Schutz der personenbezogenen Daten dienen und diese nicht gefährden, können zu jedem Zeitpunkt in einvernehmlicher Rücksprache eingesetzt werden.

1. Technische Maßnahmen:

1.1 Verschlüsselung:

- **Datenverschlüsselung:** Alle besonders schutzwürdigen personenbezogenen Daten müssen sowohl bei der Übertragung als auch bei der Speicherung mittels starker Verschlüsselungsverfahren (z.B. AES-256) geschützt werden.
- **Schlüsselspeicherung:** Verschlüsselungsschlüssel müssen sicher gespeichert und verwaltet werden.

1.2 Transportverschlüsselung:

- **TLS/SSL:** Alle Datenübertragungen müssen mindestens durch TLS (Transport Layer Security) in der aktuellen Version (z.B. TLS 1.3 oder höher) geschützt werden. Auf eigenes Risiko des Auftragnehmers kann auch TLS 1.2 verwendet werden. Der Auftragnehmer übernimmt hierbei das Risiko.
- **VPN:** Bei der Übertragung über unsichere Netzwerke ist der Einsatz von Virtual Private Networks (VPNs) erforderlich.
- **End-to-End-Verschlüsselung:** Bei besonders schutzwürdigen personenbezogenen Daten ist eine End-to-End-Verschlüsselung zu implementieren, um sicherzustellen, dass Daten nur von autorisierten Endpunkten entschlüsselt werden können.
- **E-Mail-Verschlüsselung:** E-Mails, die besonders schutzwürdige personenbezogenen Daten enthalten, müssen z.B. mit S/MIME oder PGP verschlüsselt werden.

1.3 Zutrittskontrolle:

- Physische Zugangskontrollen zu den Räumlichkeiten, in denen besonders schutzwürdige personenbezogenen Daten verarbeitet werden, z.B. durch elektronische Zugangssysteme, Sicherheitspersonal, Videoüberwachung.
- Protokollierung aller Zutrittsaktivitäten.

1.4 Zugangskontrolle:

- Implementierung von Multi-Faktor-Authentifizierung (MFA), insbesondere für den Zugang zu besonders schutzwürdigen personenbezogene Daten und zentraler Rechnerstruktur.
- Verwendung von rollenbasierter Berechtigungsvergabe zur Sicherstellung, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben.
- Regelmäßige Überprüfung und Aktualisierung von Benutzerrechten.
- Sachkundiger Einsatz von Schutzprogrammen (u.a. Virens Scanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter).

1.5 Zugriffskontrolle:

- Implementierung von Mechanismen zur Protokollierung und Überwachung von Zugriffen auf besonders schutzwürdige personenbezogene Daten.

1.6 Trennungskontrolle

- Einzelne Mandanten sind streng voneinander physisch und/oder logisch getrennt.
- Daten, auf die sich diese Zusatzvereinbarung bezieht, werden physisch und/oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung (Backups) erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

1.7 Datensicherung:

- Regelmäßige, automatisierte Backups.
- Backup- und Recovery-Konzept ist vorhanden und wird regelmäßig getestet.
- Sicherstellung, dass Backups ebenfalls verschlüsselt und sicher gespeichert werden.

1.8 Standards für Rechenzentren:

- Rechenzentren sollten mindestens die Anforderungen der ISO 27001 erfüllen.
- Rechenzentren sollten idealerweise auch die ISO 27701 erfüllen.
- Cloudservices von Rechenzentren sollten idealerweise auch die C5-Kriterien erfüllen.
- Physische Sicherheitsmaßnahmen wie u.a. Zugangskontrollen, Videoüberwachung und Brandschutzsysteme müssen implementiert sein.

2. Organisatorische Maßnahmen:

2.1 Schulung und Sensibilisierung:

- Regelmäßige Schulungen und Sensibilisierungsmaßnahmen für alle Mitarbeiter, die mit personenbezogenen Daten arbeiten, insbesondere, wenn sie mit besonders schutzwürdigen personenbezogenen Daten arbeiten.
- Dokumentation und Nachverfolgung der Teilnahme an Schulungen.

2.2 Vertraulichkeitserklärungen:

- Alle Mitarbeiter des Auftragnehmers, die Zugang zu besonders schutzwürdigen personenbezogenen Daten haben, müssen Vertraulichkeitserklärungen/Verschwiegenheitserklärungen unterzeichnen, insbesondere mit Bezug auf §203 StGB.

2.3 Datenschutzmanagement:

- Ernennung eines Datenschutzbeauftragten, der für die Einhaltung der Datenschutzbestimmungen und die Umsetzung dieser Vereinbarung verantwortlich ist.
- Durchführung regelmäßiger Datenschutz-Audits und Risikoanalysen.
- Vorhandensein eines Datenschutzmanagements, sowie mindestens gängiger Richtlinien und Policies der Informationssicherheit

2.4 Vorfallmanagement:

- Implementierung eines Verfahrens zur Erkennung, Meldung und Behandlung von Sicherheitsvorfällen.
- Verpflichtung zur unverzüglichen Benachrichtigung des Auftraggebers im Falle eines Datenschutzvorfalls.

2.5 Unterauftragnehmer:

- Eine Liste der aktuellen Unterauftragnehmer ist im Rahmen des AV-Vertrags aufzuführen.
- Der Auftragnehmer ist verpflichtet, vor der Einschaltung von Unterauftragnehmern Rücksprache mit dem Auftraggeber zu halten.
- Sicherstellung, dass Unterauftragnehmer die gleichen Datenschutz- und Sicherheitsmaßnahmen einhalten wie in dieser Vereinbarung festgelegt.
- Regelmäßige Überprüfung der Datenschutzkonformität und Sicherheitsmaßnahmen der Unterauftragnehmer.

2.6 Datenträgerentsorgung:

- Datenschutzkonforme Löschung/Vernichtung von Daten bzw. Datenträgern und Dokumenten entsprechend der Sicherheitsstufe der Daten, z.B. durch physische Zerstörung oder sichere Datenlöschung (vgl. DIN 66399, ISO/IEC 21964)
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.

Anlage 2 – Kontaktdaten des Auftragnehmers

1. Datenschutzbeauftragte(r)

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

oder

2. Ansprechpartner (wenn kein(e) Datenschutzbeauftragte(r) erforderlich ist)

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

oder

3. ständiger Vertreter gemäß Art. 27 DS-GVO

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

Anlage 3 – Liste der Unterauftragnehmer des Auftragnehmers

Alternativ in freier Form zur Verfügung stellen.

Sollten keine Unterauftragnehmer im Einsatz sein, bitte diese Seite entwerten.

Firma Unterauftragnehmer	Anschrift/Land	Leistung

Anlage 4 – Weisungsberechtigte Personen

1. beim Auftraggeber

Als weisungsberechtigte Personen im Sinne dieser Vereinbarung gelten die jeweiligen hauptverantwortlichen Fachbereichsleiter*innen am Universitätsklinikum Frankfurt oder deren stellvertretenden Personen. Das Weisungsrecht beschränkt sich auf die Hauptvereinbarung oder SLA des jeweils verantwortlichen Fachbereichs am Universitätsklinikum Frankfurt im Sinne der DSGVO mit dem Auftragnehmer.

2. beim Auftragnehmer

Herr / Frau	
Name, Vorname	
Straße	
PLZ, Ort	
Telefon	
E-Mail-Adresse	

Zuschlagskriterien und Bewertungsmatrix –Managed Services

Universitätsklinikum Frankfurt

Vergabeverfahren: Netzwerkbetrieb und Migration

1. Gesamtbewertung und Rangbildung

Die Gesamtwertungssumme eines Angebots ergibt sich aus der Summe der Punkte für Preis und Qualität. Die maximale Gesamtwertungssumme beträgt 100 Punkte. Den Zuschlag erhält das Angebot mit der höchsten Gesamtwertungssumme.

Wertungsbereich	Gewichtung	Max. P.	Min. P.
Preis (Wertungssumme über 60 Monate)	40 %	40	0
Qualität – Übernahme, Transition, Implementierung und Ramp-up	15 %	15	0
Qualität – Managed Service, Monitoring, Reporting und Automatisierung	25 %	25	0
Qualität – Eingesetztes Betriebsteam (Qualifikation und Erfahrung)	10 %	10	0
Qualität – Exit und Providerwechsel	10 %	10	0
Gesamtwertungssumme	100 %	100	0

2. Preisbewertung

2.1 Wertungssumme

Grundlage der Preisbewertung ist die Wertungssumme des Angebots. Diese umfasst die Gesamtkosten über die Vertragslaufzeit von 60 Monaten gemäß Preismatrix. Sie setzt sich aus einmaligen Kosten, laufenden Managed-Service-Kosten, Integrationsleistungen, optionalen Leistungen und den in der Preismatrix abgebildeten späteren Scope-Erweiterungen zusammen.

2.2 Bewertungsmethode (UfAB-Interpolationsmethode)

Die Preisbewertung erfolgt nach der Interpolationsmethode der UfAB. Das Angebot mit der niedrigsten Wertungssumme erhält die maximale Punktzahl von 40 Punkten. Jedes weitere Angebot wird linear in Bezug auf die niedrigste Wertungssumme bewertet. Ab einer Wertungssumme, die das Doppelte der niedrigsten Wertungssumme beträgt oder übersteigt, werden 0 Punkte vergeben.

2.3 Berechnungsformel

$$P = 40 \times (2 - \text{WS-Angebot} / \text{WS-min}), \text{ begrenzt auf } 0 \leq P \leq 40$$

Mit: WS-Angebot = Wertungssumme des zu bewertenden Angebots; WS-min = niedrigste Wertungssumme aller wertbaren Angebote.

2.4 Berechnungsbeispiel

Bieter	Wertungssumme (EUR)	Verhältnis zu WS-min	Preispunkte
Bieter A (günstigster)	10.000.000	1,00	40,00

Bieter	Wertungssumme (EUR)	Verhältnis zu WS-min	Preispunkte
Bieter B	12.000.000	1,20	32,00
Bieter C	15.000.000	1,50	20,00
Bieter D	20.000.000	2,00	0,00

Punktzahlen werden auf zwei Nachkommastellen kaufmännisch gerundet.

3. Qualitätsbewertung

3.1 Notensystem

Je Themenfeld wird genau eine der folgenden Bewertungsstufen vergeben. Zwischenwerte sind nicht zulässig. Die Punktwerte sind je Themenfeld entsprechend der jeweiligen Maximalpunktzahl festgelegt. Die Reihenfolge der Punktwerte entspricht den Themenfeldern 1 / 2 / 3 / 4 (Übernahme / Managed Service / Betriebsteam / Exit).

Bewertungsstufe	Punkte je Themenfeld	Bedeutung
Sehr gut	15 / 25 / 10 / 10	Die Darstellung ist fachlich substantiell, durchgängig begründet und zeigt belastbare Erfahrung im Betrieb kritischer Enterprise- bzw. Kliniknetzwerke. Alle Bereiche des Themenfelds sind konkret und nachvollziehbar behandelt.
Gut	12 / 20 / 8 / 8	Die Darstellung ist überwiegend konkret und nachvollziehbar. Einzelne Aspekte bleiben allgemein gehalten oder weniger ausgearbeitet.
Befriedigend	9 / 15 / 6 / 6	Die Darstellung erfüllt die Anforderungen formal. Konkrete Bezüge zum Auftraggeber und zur kritischen Betriebsumgebung sind nur stellenweise erkennbar.
Ausreichend	6 / 10 / 4 / 4	Die Darstellung deckt die Themen formal ab, bleibt aber überwiegend generisch. Einzelne wesentliche Aspekte sind nicht belastbar behandelt.
Mangelhaft	3 / 5 / 2 / 2	Wesentliche Inhalte fehlen oder bleiben unklar. Die Darstellung wirkt schablonenhaft und zeigt keine ausreichende Betriebskompetenz für den Leistungsgegenstand.
Ungenügend	0 / 0 / 0 / 0	Das Themenfeld ist nicht oder nur fragmentarisch behandelt. Inhalte sind ohne fachliche Substanz oder ohne Bezug zur Aufgabenstellung.

3.2 Bewertungsdimensionen

Die Bewertungskommission bezieht bei der Notenfindung die folgenden übergreifenden Dimensionen in die themenspezifischen Indikatoren ein:

- Fachliche Tiefe und argumentative Qualität der Darstellung.
- Konkretheit und Bezug zur bestehenden LAN-/WLAN-Infrastruktur des Auftraggebers.
- Belastbarkeit der genannten Verfahren, Erfahrungen, Rollen und Maßnahmen.

- Vollständigkeit der Behandlung der definierten Bereiche im jeweiligen Themenfeld.
- Plausibilität, Risikobewusstsein und Nachvollziehbarkeit der Schlussfolgerungen.

4. Qualitätskriterien Themenfeld 1: Übernahme, Transition, Implementierung und Ramp-up

Bewertet werden die Belastbarkeit des Vorgehens bei Service Ownership Transfer, Due Diligence, Betriebsübernahme, Anbindung an Prozesse und Tools sowie die Fähigkeit, den Übergang in den SLA-wirksamen Betrieb ohne vermeidbare Beeinträchtigung des Klinikbetriebs zu gestalten. Besonderes Gewicht erhält das Konzept für den hochverfügbaren Klinikbetrieb, die strikte Change-Koordination und die Eskalationswege während des Übergangs. Maximal erreichbar: 15 Punkte.

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 15 Punkte	SOT und Due Diligence sind konkret, risikoorientiert und auf eine bestehende Cisco-basierte Enterprise-LAN-/WLAN-Umgebung zugeschnitten. Umgang mit unvollständiger Dokumentation, Altdienstleister-Abhängigkeiten und kritischen Betriebsrisiken ist nachvollziehbar beschrieben. Ramp-up, Ressourcen, Cut-over, SLA-Start und Abnahmegates sind mit klaren Entscheidungspunkten dargestellt. ServiceNow-, Monitoring-, Zugangs- und Eskalationsintegration sind konkret geplant. Der Bieter beschreibt realistische Übergangs- und Unterstützungsoptionen für den Zeitraum zwischen Zuschlag, Betriebsübernahme und SLA-Start. Zusätzliche Business Units bzw. spätere Scope-Erweiterungen werden über ein standardisiertes Aufnahmeverfahren berücksichtigt.
Gut 12 Punkte	Vorgehen ist überwiegend konkret und nachvollziehbar. SOT, Ramp-up und Abnahme sind plausibel beschrieben; einzelne Entscheidungspunkte oder Abhängigkeiten bleiben weniger präzise. Tool- und Prozessintegration sind grundsätzlich tragfähig. Risiken des Klinikbetriebs sind erkennbar adressiert.
Befriedigend 9 Punkte	Vorgehen erfüllt die Anforderungen formal, bleibt aber in Teilen generisch. SOT und Due Diligence sind beschrieben, jedoch ohne ausreichende Tiefe zu Dokumentationslücken, Bestandsrisiken oder SLA-Start. Ramp-up und Ressourcenplanung sind nur grob erkennbar.
Ausreichend 6 Punkte	Konzept deckt die Themen formal ab, bleibt aber oberflächlich. Wesentliche Aspekte wie Toolanbindung, Monitoringübernahme, Abnahmegates, Rückfallverfahren oder klinische Sperrzeiten sind nicht belastbar behandelt.
Mangelhaft 3 Punkte	Wesentliche Inhalte fehlen oder sind widersprüchlich. Übernahme wirkt wie allgemeines Projektvorgehen ohne belastbare SOT-Logik. Risiken für den laufenden Klinikbetrieb werden nicht ausreichend beherrscht.
Ungenügend 0 Punkte	Themenfeld nicht oder nur fragmentarisch behandelt. Keine erkennbare Fähigkeit zur geordneten Betriebsübernahme.

5. Qualitätskriterien Themenfeld 2: Managed Service, Monitoring, Reporting und Automatisierung

Bewertet werden Tragfähigkeit des Betriebsmodells, Cisco-Bestandsbetrieb, NOC-/Service-Desk-Struktur, ITSM-Integration, Incident-/Problem-/Change-/Release-Prozesse, Monitoring, Reporting, Lifecycle-Management, Automatisierung und kontinuierliche Verbesserung.

Bewertungsschwerpunkt ist die Tragfähigkeit des Betriebs für ein Verfügbarkeits- und betriebskritisches Kliniknetz, einschließlich strikter Change-Koordination und belastbarer Eskalation. Maximal erreichbar: 25 Punkte.

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 25 Punkte	Betriebsorganisation ist klar, rollenbasiert und für kritische LAN-/WLAN-Services belastbar beschrieben. Cisco-Bestandsbetrieb, 2nd-/3rd-Level-Support, Vertretung und Herstellereskalation sind nachvollziehbar abgesichert. Incident-, Problem-, Change- und Release-Prozesse sind ITIL-nah, klinikbetrieblich tragfähig und in ServiceNow integrierbar. Monitoring und Observability liefern qualifizierte Events statt Ticket-Spam; Topologie-, Abhängigkeits- und Priorisierungslogik sind beschrieben. Reporting ist operativ und strategisch verwertbar, einschließlich SLA, Trends, Lifecycle, EoL/EoS, Change-Qualität und Verbesserungsmaßnahmen. Automatisierung wird sinnvoll begrenzt, changefähig, protokolliert und rückrollbar dargestellt. CMDB, Dokumentation, Konfigurationssicherung und FMO-Überführung sind konsistent beschrieben.
Gut 20 Punkte	Betriebsmodell ist überwiegend konkret und tragfähig. NOC, Rollen, Monitoring, Reporting und ITSM-Prozesse sind plausibel beschrieben. Einzelne Aspekte wie Automatisierungsgrenzen, CMDB-Qualität, Lifecycle-Priorisierung oder Eventkorrelation bleiben weniger ausgearbeitet.
Befriedigend 15 Punkte	Betriebsmodell erfüllt die Anforderungen formal. Monitoring, Reporting und ITSM-Prozesse sind vorhanden, aber teilweise generisch. Cisco-spezifische Betriebskompetenz und Umgang mit Legacy-/EoS-Komponenten sind nicht durchgängig belastbar dargestellt.
Ausreichend 10 Punkte	Konzept benennt die Betriebsleistungen, bleibt aber überwiegend beschreibend. Eventkorrelation, Reportingqualität, Problem Management, Lifecycle-Steuerung und Automatisierung sind nur oberflächlich behandelt.
Mangelhaft 5 Punkte	Wesentliche Inhalte fehlen. Betriebsorganisation, Eskalation, Monitoring oder Change-Qualität sind nicht belastbar. Kein ausreichender Bezug zur bestehenden LAN-/WLAN-Infrastruktur und deren Kritikalität.
Ungenügend 0 Punkte	Themenfeld nicht oder nur fragmentarisch behandelt. Keine nachvollziehbare Managed-Service-Fähigkeit.

6. Qualitätskriterien Themenfeld 3: Eingesetztes Betriebsteam (Qualifikation und Erfahrung)

Bewertet werden Qualifikation, Zertifizierung und einschlägige Betriebserfahrung der rollenscharf benannten Personen, die im Vertrag tatsächlich eingesetzt werden (NOC, 2nd-/3rd-Level-Support, Netzwerkarchitektur, Monitoring, Change-/Release-Management, Service Delivery Management), soweit die Qualität dieses Personals das Niveau der Auftragsausführung erheblich beeinflusst. Gegenstand der Bewertung ist das konkrete Einsatzteam, nicht die Unternehmensgröße. Die in den Eignungsanforderungen geforderten Mindestzertifizierungen bleiben hiervon unberührt und werden nicht erneut bewertet. Maximal erreichbar: 10 Punkte.

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 10 Punkte	Das eingesetzte Team ist rollenscharf benannt; die Cisco-Enterprise-Qualifikationen (CCNP/CCIE) sind den konkreten Schlüsselrollen zugeordnet. Einschlägige Betriebserfahrung in verfügbarkeitskritischen Klinik- bzw. KRITIS-Netzen ist je Schlüsselrolle belastbar dargestellt. Vertretungs- und Eskalationsbesetzung sind lückenlos; Verfügbarkeit und Bindung der benannten Personen an den Auftrag sind nachvollziehbar.
Gut 8 Punkte	Team überwiegend rollenscharf benannt, Qualifikationen plausibel den Rollen zugeordnet. Einzelne Schlüsselrollen, Vertretungsregelungen oder Erfahrungsnachweise bleiben weniger konkret.
Befriedigend 6 Punkte	Qualifikationen sind formal nachgewiesen, der Bezug zur konkreten Rolle und zum kritischen Klinikbetrieb bleibt jedoch teilweise generisch. Die Erfahrungstiefe ist nur grob erkennbar.
Ausreichend 4 Punkte	Team und Qualifikationen sind benannt, bleiben aber überwiegend allgemein. Schlüsselrollen, Vertretung oder einschlägige Kritikalitätserfahrung sind nicht belastbar behandelt.
Mangelhaft 2 Punkte	Wesentliche Angaben fehlen oder bleiben unklar. Qualifikationen werden ohne Rollenbezug aufgeführt; ein belastbarer Bezug zum kritischen Netzbetrieb fehlt.
Ungenügend 0 Punkte	Themenfeld nicht oder nur fragmentarisch behandelt. Keine nachvollziehbare Aussage zum eingesetzten Betriebsteam.

7. Qualitätskriterien Themenfeld 4: Exit und Providerwechsel

Bewertet wird, ob der Bieter Providerwechselfähigkeit nicht erst am Vertragsende, sondern über die gesamte Vertragslaufzeit sicherstellt. Maximal erreichbar: 10 Punkte.

Bewertungsstufe	Themenspezifische Indikatoren
Sehr gut 10 Punkte	Exit-Fähigkeit ist als laufendes Betriebsprinzip beschrieben. Betriebshandbuch, CMDB, Konfigurationssicherungen, Monitoringlogik, Runbooks, Known Errors, offene Tickets, Risiken und SLA-Historie sind übergabefähig strukturiert. Exit-Plan, Übergabeobjekte, Fristen, Workshops, Unterstützung eines Nachfolgeproviders und Abschlusskriterien sind konkret und prüfbar. Datenrückgabe, Löschung, Exportformate, Rechte an Betriebsdokumentation und Vermeidung von Tool-/Provider-Lock-in sind nachvollziehbar geregelt.
Gut 8 Punkte	Exit-Konzept ist plausibel und weitgehend vollständig. Einzelne Übergabeobjekte, Fristen oder Exportmechanismen bleiben weniger konkret. Laufende Exit-Fähigkeit ist erkennbar, aber nicht durchgängig operationalisiert.
Befriedigend 6 Punkte	Exit ist formal beschrieben. Es fehlen jedoch belastbare Aussagen zu laufender Dokumentationsqualität, Konfigurations- und CMDB-Exporten, Nachfolgeprovider-Unterstützung oder Abschlusskriterien.
Ausreichend 4 Punkte	Exit wird überwiegend als Vertragsendphase verstanden. Laufende Providerwechselfähigkeit und konkrete Übergabeartefakte sind nur oberflächlich dargestellt.

Bewertungsstufe	Themenspezifische Indikatoren
Mangelhaft 2 Punkte	Wesentliche Exit-Inhalte fehlen oder bleiben unklar. Erkennbares Risiko von Wissensverlust oder Provider-Lock-in.
Ungenügend 0 Punkte	Themenfeld nicht oder nur fragmentarisch behandelt. Keine belastbare Exit-Fähigkeit.

8. Ranggleichheit und Verfahrenshinweise

8.1 Auflösung von Ranggleichheit

Erreichen mehrere Angebote nach Anwendung der Bewertungsmethodik dieselbe Gesamtwertungssumme, wird der Zuschlag in folgender Reihenfolge bestimmt:

Vorrang erhält das Angebot mit der höheren Qualitäts-Punktzahl.

Besteht weiterhin Ranggleichheit, erhält das Angebot Vorrang, das im Themenfeld 2 „Managed Service, Monitoring, Reporting und Automatisierung“ die höhere Punktzahl erreicht hat.

Besteht weiterhin Ranggleichheit, erhält das Angebot Vorrang, das im Themenfeld 1 „Übernahme, Transition, Implementierung und Ramp-up“ die höhere Punktzahl erreicht hat.

Besteht weiterhin Ranggleichheit, entscheidet das Los unter Aufsicht des Auftraggebers.

Anforderungen an die Lösungsansätze

1. Vorbemerkung

Mit dem Angebot ist ein schriftliches Lösungs- und Umsetzungskonzept einzureichen, das die in diesem Dokument benannten Themenfelder vollständig abdeckt. Das Konzept dient dem Auftraggeber als Grundlage für die qualitative Bewertung des Angebots.

Erwartet wird eine fachlich begründete Darstellung mit konkretem Bezug zur bestehenden LAN-/WLAN-Infrastruktur des Auftraggebers, zur Betriebsübernahme, zum CMO-Betrieb, zur späteren Integration bereitgestellter Komponenten und zur Providerwechselfähigkeit. Eine reine Aufzählung von Herstellerfunktionen oder generische Standarddarstellungen werden geringer bewertet.

Der Bieter strukturiert seinen Beitrag in der Reihenfolge der Themenfelder und der dort definierten Bereiche. Inhaltliche Bezüge zur Leistungsbeschreibung Anlage L sind explizit zu kennzeichnen. Querverweise zwischen Themenfeldern sind zulässig, soweit sie Redundanzen vermeiden und die Bewertung nicht erschweren.

2. Formale Anforderungen an das Konzept

Kriterium	Vorgabe
Schriftart	Calibri oder Arial
Schriftgröße	11 pt Fließtext; 9-10 pt zulässig in Tabellen und Beschriftungen
Zeilenabstand	1,15-fach, einfacher Zeichenabstand, normal
Seitenränder	links 2,5 cm, rechts 2,5 cm, oben 2,5 cm, unten 2,0 cm
Papierformat	DIN A4, einseitig bedruckt
Seitennummerierung	Fortlaufend, in der Fußzeile
Abbildungen / Schaubilder	Im Rahmen der maximalen Seitenanzahl zulässig; Lesbarkeit mindestens 9 pt ist sicherzustellen
Inhaltsverzeichnis	Erforderlich; zählt nicht in die Seitenobergrenzen ein
Dateiformat	PDF, durchsuchbar, nicht passwortgeschützt
Sprache	Deutsch

Die folgenden Seitenobergrenzen sind je Themenfeld einzuhalten. Inhaltsverzeichnis, Deckblatt und Anlagen werden nicht eingerechnet.

Nr.	Themenfeld	Max. Seiten
1	Übernahme, Transition, Implementierung und Ramp-Up	8 Seiten
2	Managed Services, Monitoring, Reporting und Automatisierung	12 Seiten
3	Eingesetztes Betriebsteam (Qualifikation und Erfahrung)	4 Seiten
4	Exit und Providerwechsel	6 Seiten
	Summe ohne Deckblatt, Inhaltsverzeichnis und Anlagen	max. 30 Seiten

3. Bewertungsgrundlage

Die qualitative Bewertung des Konzepts erfolgt anhand der vier Themenfelder. Die Bewertungssystematik, das Notensystem sowie die Indikatoren sind im Dokument "Zuschlagskriterien und Bewertungsmatrix" detailliert beschrieben.

Wertungsbereich	Gewichtung	Max. Punkte
Preis (Wertungssumme)	40 %	40
Qualität - Themenfeld 1 (Übernahme, Transition, Implementierung und Ramp-Up)	15 %	15
Qualität - Themenfeld 2 (Managed Services, Monitoring, Reporting und Automatisierung)	25 %	25
Qualität - Themenfeld 3 (Eingesetztes Betriebsteam – Qualifikation und Erfahrung)	10 %	10
Qualität - Themenfeld 4 (Exit und Providerwechsel)	10 %	10
Summe	100 %	100

4. Themenfeld 1: Übernahme, Transition, Implementierung und Ramp-Up

4.1 Ziel

Der Auftraggeber bewertet, wie belastbar der Bieter den Übergang vom bisherigen Betrieb in den Managed Service, die Service Ownership Transfer Phase, die Due Diligence des Bestands, den Ramp-Up der Betriebsorganisation und den Übergang in den SLA-wirksamen Betrieb beherrscht. Bewertet wird insbesondere, ob der Klinikbetrieb während der Übergangsphase stabil bleibt und ob Risiken frühzeitig erkannt und gesteuert werden.

4.2 Inhaltliche Erwartung

Der Bieter strukturiert seinen Beitrag zu diesem Themenfeld anhand der nachfolgenden Bereiche. Beizufügen ist ein Projekt- und Meilensteinplan, der Phasen, Entscheidungspunkte, Abhängigkeiten, Ressourcen, Mitwirkungen des Auftraggebers und Abnahmekriterien abbildet.

A. Service Ownership Transfer und Due Diligence

Der Bieter erläutert sein Vorgehen bei der Übernahme der bestehenden LAN-/WLAN-Infrastruktur vom bisherigen Betrieb bzw. Altdienstleister. Dabei ist insbesondere darzustellen, wie Dokumentation, Zugänge, Assetlisten, Netzpläne, Konfigurationen, Monitoringinformationen, offene Tickets und bekannte Risiken übernommen und geprüft werden.

Der Bieter beschreibt, wie er mit unvollständiger, veralteter oder widersprüchlicher Dokumentation umgeht und wie er betriebsverhindernde, risikorelevante und dokumentationsrelevante Lücken unterscheidet.

Der Bieter stellt dar, wie der vorhandene Cisco-Bestand fachlich bewertet und in den CMO-Betrieb überführt wird.

B. Ramp-Up, Cut-Over und SLA-Start

Der Bieter beschreibt sein Ramp-Up-Modell einschließlich Projektleitung, Schlüsselrollen, 2nd-/3rd-Level-Ressourcen, Vertretungsregelungen, Eskalationswegen und zeitlicher Verfügbarkeit.

Der Bieter erläutert die Kriterien für den Übergang in den SLA-wirksamen Betrieb und benennt Abnahmegates, Testfälle und Mindestvoraussetzungen für den Betriebsstart.

Der Bieter beschreibt seinen Umgang mit einem möglichen Übergangszeitraum zwischen Zuschlag, technischer Betriebsübernahme und vollständigem SLA-Start. Optionale Übergangs- oder Unterstützungsleistungen sind klar von regulären Managed-Services-Leistungen abzugrenzen.

C. Prozess-, Tool- und Monitoringintegration

Der Bieter erläutert, wie ServiceNow des Auftraggebers als führendes Ticketsystem eingebunden wird und wie Ticketfluss, Statussynchronisation, Pflichtfelder, Eskalation und Abschlussdokumentation umgesetzt werden.

Der Bieter beschreibt, wie vorhandene oder neue Monitoringinformationen übernommen, qualifiziert und in ein handlungsfähiges Betriebsmonitoring überführt werden.

Der Bieter stellt dar, wie administrative Zugänge eingerichtet, abgesichert, protokolliert und in das Berechtigungskonzept des Auftraggebers eingebunden werden.

D. Integrationsvorgehen und spätere Scope-Erweiterungen

Der Bieter beschreibt sein Verfahren zur Integration bereitgestellter oder separat beschaffter Komponenten in den Managed Service, einschließlich Vorprüfung, Planung, Konfiguration, Test, Dokumentation, Monitoring, CMDB-Pflege und formaler Betriebsübernahme.

Der Bieter erläutert sein standardisiertes Verfahren zur Aufnahme zusätzlicher Standorte, Business Units oder Netzbereiche in den Leistungsumfang. Dies umfasst Bestandsaufnahme, Risikoprüfung, Aufwandsschätzung, Integration, Dokumentation und Abnahme.

Der Bieter berücksichtigt, dass der Bestand Sachsenhausen zeitversetzt in den Managed Service überführt werden kann und vom initialen UKF-Campusbetrieb abzugrenzen ist.

E. Risiko-, Kommunikations- und Wissensmanagement

Der Bieter erläutert, wie er Risiken für klinisch-kritische Bereiche, zentrale Netzfunktionen, WLAN, NAC-/AAA-Schnittstellen, passive Abhängigkeiten und EoL-/EoS-Komponenten während der Übernahme erkennt und steuert.

Der Bieter beschreibt Kommunikationswege, Eskalationslogik, Regeltermine und Managementeskalation während der SOT- und Ramp-Up-Phase.

Der Bieter stellt sein Vorgehen zum Wissenstransfer, zur Erstellung des initialen Betriebshandbuchs und zur formalen Betriebsübergabe dar.

5. Themenfeld 2: Managed Services, Monitoring, Reporting und Automatisierung

5.1 Ziel

Der Auftraggeber bewertet die Tragfähigkeit des Betriebsmodells über die Vertragslaufzeit. Bewertet werden Cisco-Bestandsbetrieb, NOC-/Service-Desk-Modell, 2nd-/3rd-Level-Unterstützung, Prozessqualität, Monitoring, Reporting, Lifecycle-Steuerung, Automatisierung, Dokumentation und kontinuierliche Verbesserung.

5.2 Inhaltliche Erwartung

A. Betriebsorganisation und Serviceverantwortung

Der Bieter beschreibt seine Betriebsorganisation einschließlich NOC bzw. Service Desk, Service Delivery Management, technischer Betriebsverantwortung, Incident-, Problem-, Change-, Release-, Lifecycle- und Dokumentationsrollen.

Der Bieter erläutert, wie er qualifizierte Cisco-Betriebsfähigkeit für Switching, Routing, WLAN-Controller, Access Points, Managementsysteme, Konfigurationssicherung, Troubleshooting und Herstellereskalation sicherstellt.

Der Bieter stellt dar, wie Personalwechsel, Urlaub, Krankheit, Lastspitzen und Schlüsselrollen über die Vertragslaufzeit abgesichert werden.

B. Incident-, Problem-, Change- und Release-Management

Der Bieter beschreibt seinen Incident-Prozess einschließlich Annahme, Vorqualifizierung, Priorisierung, technischer Analyse, Eskalation, Wiederherstellung, Abschlussdokumentation und Major-Incident-Steuerung.

Der Bieter erläutert, wie er wiederkehrende Störungen identifiziert, Problems eröffnet, Root-Cause-Analysen durchführt, Known Errors pflegt und Präventionsmaßnahmen nachverfolgt.

Der Bieter beschreibt sein Change- und Release-Management für produktive Netzwerkänderungen, einschließlich Risiko-/Impactbewertung, CAB-Einbindung, Test, Rollback, Wartungsfenster, Emergency Changes und Change-Kennzahlen.

C. Monitoring, Observability und Reporting

Der Bieter erläutert seinen Monitoringansatz für Core, Distribution, Access, WLAN, Managementsysteme, NAC-/AAA-Schnittstellen, Uplinks, kritische Standortverbindungen, Konfigurationsänderungen und sicherheitsrelevante Systemmeldungen.

Der Bieter beschreibt, wie technische Einzelereignisse korreliert, priorisiert und so verarbeitet werden, dass Ticket-Spam vermieden wird und der Auftraggeber handlungsfähige Betriebsinformationen erhält.

Der Bieter stellt sein Reportingkonzept dar. Es muss mindestens SLA, Verfügbarkeit, Ticketvolumen, Major Incidents, Problems, Changes, Lifecycle, EoL/EoS, Kapazität, Performance, Risiken, Verbesserungsmaßnahmen und offene Mitwirkungspunkte umfassen.

Der Bieter erläutert, welche Dashboards oder lesenden Sichten dem Auftraggeber bereitgestellt werden und wie Transparenz ohne unkontrollierte Änderungsmöglichkeit sichergestellt wird.

D. Lifecycle-, EoL-/EoS-, RMA- und Sicherheitsmanagement

Der Bieter beschreibt, wie Supportstatus, EoL-/EoS-Daten, Firmwarestände, Security Advisories, Ersatzteilrisiken und betriebliche Risiken laufend überwacht, bewertet, priorisiert und berichtet werden.

Der Bieter erläutert seine Rolle bei RMA-Fällen, Herstellereskalationen, Ersatzteilkoordination, Wiederinbetriebnahme und Dokumentation, ohne eine verdeckte Hardwarelieferverpflichtung zu unterstellen.

Der Bieter stellt dar, wie Security Incidents mit Netzwerkbezug erkannt, bewertet, an die Sicherheitsrollen des Auftraggebers gemeldet und mit SOC/SIEM, Informationssicherheit und Datenschutz abgestimmt werden.

E. Automatisierung, CMDB, Dokumentation und kontinuierliche Verbesserung

Der Bieter erläutert, welche Betriebsaufgaben automatisiert oder teilautomatisiert werden können, z. B. Konfigurationssicherung, Firmware-Compliance, Portprofile, Monitoring, CMDB-Abgleich oder Reporting.

Der Bieter beschreibt, wie automatisierte Änderungen kontrolliert, freigegeben, protokolliert, getestet und rückrollbar umgesetzt werden. Unkontrollierte Automatisierung im produktiven Kliniknetz ist auszuschließen.

Der Bieter stellt sein Vorgehen zur Pflege von CMDB, Betriebshandbuch, Konfigurationssicherungen, SOPs, Runbooks, Knowledge Base und Known-Error-Informationen dar.

Der Bieter beschreibt, wie kontinuierliche Verbesserung aus Service Reports, Trends, Incidents, Problems, Changes und Lifecycle-Informationen abgeleitet und gesteuert wird.

6. Themenfeld 3: Eingesetztes Betriebsteam (Qualifikation und Erfahrung)

6.1 Ziel

Der Auftraggeber bewertet Qualifikation, Zertifizierung und einschlägige Betriebserfahrung der rollenscharf benannten Personen, die im Vertrag tatsächlich eingesetzt werden (NOC, 2nd-/3rd-Level-Support, Netzwerkarchitektur, Monitoring, Change-/Release-Management, Service Delivery Management), soweit die Qualität dieses Personals das Niveau der Auftragsausführung erheblich beeinflusst. Gegenstand der Bewertung ist das konkrete Einsatzteam, nicht die Unternehmensgröße. Die in den Eignungsanforderungen geforderten

Mindestzertifizierungen (insbesondere CCNP Enterprise und CCIE Enterprise Infrastructure) bleiben hiervon unberührt und werden nicht erneut bewertet.

6.2 Inhaltliche Erwartung

Der Bieter strukturiert seinen Beitrag zu diesem Themenfeld anhand der nachfolgenden Bereiche. Die Darstellung erfolgt rollenscharf und mit konkretem Bezug zum Verfügbarkeits- und betriebskritischen Klinikbetrieb.

A. Rollenscharfe Teamaufstellung

Der Bieter benennt die im Vertrag tatsächlich vorgesehenen Schlüsselrollen (u. a. Service Delivery Management, technische Betriebsverantwortung Netzwerk, NOC/Service Desk, 2nd-/3rd-Level-Support, Netzwerkarchitektur, Monitoring, Incident-, Problem-, Change-/Release- und Lifecycle-Verantwortung) und ordnet ihnen die konkret eingeplanten Personen zu.

B. Qualifikation und Zertifizierung

Der Bieter ordnet die Cisco-Enterprise-Qualifikationen (CCNP Enterprise, CCIE Enterprise Infrastructure) den konkreten Schlüsselrollen zu und benennt mindestens einen Technical Lead. Die Zuordnung muss nachvollziehbar machen, welche Person welche Betriebsverantwortung mit welcher Qualifikation trägt.

C. Einschlägige Betriebserfahrung

Der Bieter stellt je Schlüsselrolle die einschlägige, belastbare Betriebserfahrung im Betrieb verfügbarkeitskritischer Klinik-, KRITIS- oder vergleichbar kritischer Enterprise-Netzwerke dar, einschließlich Erfahrung mit Cisco-Enterprise-Switching/-Routing, WLAN-/Controllerbetrieb, NAC-/AAA-Schnittstellen sowie Change-/Release-Prozessen in produktiven kritischen Umgebungen.

D. Vertretung, Verfügbarkeit und Bindung

Der Bieter beschreibt die Vertretungs- und Eskalationsbesetzung der Schlüsselrollen und weist nach, dass kritische Störungen nicht von einzelnen Personen abhängen. Darzustellen sind Verfügbarkeit und Bindung der benannten Personen an den Auftrag über die Vertragslaufzeit.

E. Fluktuations- und Wissensmanagement

Der Bieter stellt dar, wie Personalwechsel, Urlaub, Krankheit und Fluktuation ohne Leistungsminderung bewältigt werden und wie Wissenstransfer, Dokumentationsaktualisierung und geordnete Übergabe offener Themen bei Rollenwechseln sichergestellt werden.

7. Themenfeld 4: Exit und Providerwechsel

7.1 Ziel

Der Auftraggeber bewertet, wie belastbar der Bieter die Providerwechselfähigkeit während der gesamten Vertragslaufzeit sicherstellt und wie eine geordnete Übergabe am Vertragsende oder bei vorzeitiger Vertragsbeendigung erfolgen kann.

7.2 Inhaltliche Erwartung

A. Laufende Exit-Fähigkeit

Der Bieter erläutert, wie Dokumentation, CMDB, Konfigurationen, Monitoringlogiken, Runbooks, SOPs, Known Errors, Risiken und offene Vorgänge während des Betriebs so geführt werden, dass ein späterer Providerwechsel ohne erneute vollständige Bestandsaufnahme möglich ist.

Der Bieter beschreibt, wie der Auftraggeber laufend Zugriff auf exit-relevante Betriebsinformationen erhält und wie deren Aktualität sichergestellt wird.

B. Formale Exit-Phase und Übergabeobjekte

Der Bieter beschreibt seinen Exit-Plan einschließlich Zeitplan, Rollen, Übergabeobjekten, Datenexporten, Workshops, Parallelbetriebsregelungen, offenen Risiken und Abschlusskriterien.

Der Bieter benennt mindestens folgende Übergabeobjekte: Betriebshandbuch, Netzwerkdokumentation, CMDB-/Asset-Export, Konfigurationssicherungen, Monitoring- und Alarmierungslogik, Known-Error-Auszug, offene Incidents/Problems/Changes/Risiken, Lifecycle- und EoL-/EoS-Übersicht, Service Reports, SLA-Historie, Zugriffs- und Berechtigungsdokumentation sowie Runbooks und SOPs.

C. Unterstützung des Nachfolgeproviders

Der Bieter erläutert, wie er den Auftraggeber oder einen Nachfolgeprovider durch Übergabeworkshops, technische Erläuterungen, Klärung offener Fragen, Unterstützung bei Testzugriffen und Abstimmung offener Risiken unterstützt.

Der Bieter beschreibt, wie offene Tickets, Changes, Problems und Risiken in einen geordneten Übergabezustand gebracht werden.

D. Datenrückgabe, Löschung und Lock-in-Vermeidung

Der Bieter erläutert, in welchen Formaten Betriebsdaten, Dokumentation, Konfigurationen, Reports und CMDB-Informationen exportiert werden können.

Der Bieter beschreibt, wie Daten des Auftraggebers nach Vertragsende zurückgegeben oder gelöscht werden und wie die Löschung nachvollziehbar bestätigt wird.

Der Bieter stellt dar, wie vermieden wird, dass betriebsrelevantes Wissen ausschließlich in nicht übergabefähigen internen Systemen, persönlichen Notizen oder proprietären Werkzeugen verbleibt.

8. Hinweise zur Erstellung des Konzepts

Konzepte sind in der Reihenfolge der Themenfelder 1 bis 4 zu strukturieren. Eine Untergliederung anhand der vorgegebenen Bereiche wird erwartet.

Die Leitfragen geben die fachliche Erwartung an die inhaltliche Tiefe der Darstellung vor. Erwartet wird eine argumentativ begründete Darstellung, keine reine Stichwort-Wiedergabe.

Die Besonderheiten des Auftraggebers, insbesondere Klinikbetrieb, Kritikalität, bestehende Cisco-Infrastruktur, CMO/FMO-Abgrenzung, spätere Scope-Erweiterungen und Providerwechselfähigkeit, sind konkret zu berücksichtigen.

Reine Marketing-Aussagen, Produktbroschüren und Zertifikatsabschriften sind nicht Teil des Konzepts und werden in der Bewertung nicht berücksichtigt.

Inhaltliche Bezüge zur Leistungsbeschreibung Anlage L sind explizit zu kennzeichnen. Abweichungen vom beschriebenen Leistungsumfang sind transparent darzustellen.

Die Detailbewertung der Konzepte ist im Dokument "Zuschlagskriterien und Bewertungsmatrix" geregelt.



(Nachfolgend Auftraggeber oder UKF)

Ausschreibung

"Netzwerkbetrieb und Migration"

Anlage L – Leistungsbeschreibung und Anforderungen

„Managed-Services-LAN“

Inhaltsverzeichnis

ABKÜRZUNGSVERZEICHNIS	8
1 PRÄAMBEL UND LEISTUNGSGEGENSTAND	9
1.1 AUSGANGSSITUATION.....	9
1.2 ZIEL DER AUSSCHREIBUNG.....	9
1.3 LEISTUNGSGEGENSTAND	9
1.4 VERBINDLICHE KOMPETENZANFORDERUNG FÜR CISCO-BESTANDSBETRIEB	10
1.5 GRUNDSÄTZE DER LEISTUNGSERBRINGUNG.....	10
2 BETRIEBSPHASEN UND ZIELMODELL	11
2.1 PHASENÜBERSICHT	11
2.2 SERVICE OWNERSHIP TRANSFER (SOT)	11
2.3 CURRENT MODE OF OPERATION (CMO)	11
2.4 STABILISIERUNG UND ZIELBILDPLANUNG	12
2.5 INTEGRATIONS- UND MODERNISIERUNGSPHASE	12
2.6 FUTURE MODE OF OPERATION (FMO)	12
2.7 EXIT-PHASE	12
3 LEISTUNGSUMFANG, SCOPE UND ABGRENZUNG.....	13
3.1 IM SCOPE BEFINDLICHE LEISTUNGEN.....	13
3.2 NICHT IM REGULÄREN SCOPE BEFINDLICHE LEISTUNGEN.....	13
3.3 SCHNITTSTELLEN ZU SEPARATEN HARDWAREBESCHAFFUNGEN	13
3.4 STANDORT- UND SCOPE-ERWEITERUNGEN.....	14
4 TECHNISCHE SYSTEMLANDSCHAFT - IST-ZUSTAND.....	15
4.1 GESAMTÜBERBLICK.....	15
4.2 CORE- UND BACKBONE-BEREICH	15
4.3 TOPOLOGIE, DISTRIBUTION UND ACCESS.....	15
4.4 WLAN-INFRASTRUKTUR.....	15
4.5 VERKABELUNG UND PASSIVE ABHÄNGIGKEITEN.....	16
4.6 BETRIEB, MANAGEMENT UND DOKUMENTATION.....	16
4.7 NAC, AAA UND SECURITY-SCHNITTSTELLEN	16
4.8 EINGESETZTE AKTIVE NETZWERKKOMPONENTEN IM UKF-BESTAND	17
4.9 SPÄTER EINZUBEZIEHENDER BESTAND SACHSENHAUSEN	17
4.10 LIFECYCLE- UND EoS-RELEVANTE KOMPONENTEN	18
4.10.1 UKF-CAMPUS FRANKFURT	18
4.10.2 SACHSENHAUSEN.....	18
4.11 HINWEIS ZUR BEREITSTELLUNG DETAILLIERTER ASSET-INFORMATIONEN	19

5 ZIELBILD DES MANAGED-SERVICE-BETRIEBS.....	19
5.1 BETRIEBSZIELBILD	19
5.2 ZIELBILD FÜR STANDARDISIERUNG	19
5.3 ZIELBILD FÜR AUTOMATISIERUNG.....	19
5.4 ZIELBILD FÜR SEGMENTIERUNG UND ZUGRIFFSKONTROLLE	20
5.5 ZIELBILD FÜR PROVIDERWECHSELFÄHIGKEIT	20
6 TECHNISCHE LEITPLANKEN FÜR BETRIEBS- UND INTEGRATIONSFÄHIGKEIT	21
6.1 ZWECK DER TECHNISCHEN LEITPLANKEN	21
6.2 ALLGEMEINE ANFORDERUNGEN AN ZU BETREIBENDE KOMPONENTEN	21
6.3 CORE- UND DISTRIBUTIONSEBENE.....	21
6.4 ACCESS-EBENE.....	21
6.5 WLAN-KOMPONENTEN.....	22
7 SERVICE OWNERSHIP TRANSFER UND DUE DILIGENCE.....	23
7.1 ZIELSETZUNG DER SOT-PHASE.....	23
7.2 INFORMATIONÜBERNAHME	23
7.3 SOT-ARBEITSPAKETE.....	23
7.4 SOT-ERGEBNISDOKUMENTE	23
7.5 ABNAHME DER BETRIEBSÜBERNAHME.....	24
8 MANAGED-SERVICE-GRUNDLEISTUNGEN.....	25
8.1 BETRIEBSVERANTWORTUNG	25
8.2 SERVICE DESK UND NOC.....	25
8.3 SERVICE REQUEST MANAGEMENT.....	25
8.4 VOR-ORT-UNTERSTÜTZUNG	26
8.5 KONTINUIERLICHE VERBESSERUNG	26
9 ITSM, SERVICENOW UND PROZESSINTEGRATION.....	27
9.1 FÜHRENDES TICKETSYSTEM.....	27
9.2 TICKETFLUSS.....	27
9.3 STATUSSYNCHRONISATION	27
9.4 CMDB-INTEGRATION	27
9.5 PROZESSQUALITÄT	28
10 MONITORING, OBSERVABILITY UND REPORTING	28
10.1 ZIEL DES MONITORINGS	28
10.2 MONITORINGUMFANG	28
10.3 MINDESTMETRIKEN	28
10.4 EVENTKORRELATION UND TICKET-SPAM-VERMEIDUNG	28

10.5 REPORTING.....	29
10.6 DASHBOARDS UND TRANSPARENZ	29
<u>11 INCIDENT MANAGEMENT.....</u>	30
11.1 ZIEL	30
11.2 INCIDENTANNAHME	30
11.3 PRIORISIERUNG.....	30
11.4 MAJOR INCIDENT	30
11.5 ABSCHLUSS UND DOKUMENTATION	31
<u>12 PROBLEM MANAGEMENT.....</u>	32
12.1 ZIEL	32
12.2 PROBLEMKLASSIFIKATION	32
12.3 ROOT-CAUSE-ANALYSE.....	32
12.4 KNOWN-ERROR-DATABASE.....	32
12.5 TRENDANALYSE.....	32
<u>13 CHANGE- UND RELEASE-MANAGEMENT</u>	33
13.1 CHANGE MANAGEMENT - ZIEL	33
13.2 VERFAHRENSARTEN UND CHANGE-TYPEN	33
13.3 MINDESTINHALT EINES CHANGE-ANTRAGS.....	33
13.4 CAB UND FREIGABEN	33
13.5 RELEASE MANAGEMENT	33
13.6 CHANGE-KENNZAHLEN	34
<u>14 CONFIGURATION MANAGEMENT, CMDB UND DOKUMENTATION</u>	35
14.1 GRUNDSATZ.....	35
14.2 CMDB-PFLICHTINFORMATIONEN.....	35
14.3 BETRIEBSHANDBUCH.....	35
14.4 KONFIGURATIONSSICHERUNG.....	35
14.5 KNOWLEDGE MANAGEMENT	36
<u>15 SECURITY, ZUGRIFF UND SCHNITTSTELLEN ZU SICHERHEITSPROZESSEN</u>	37
15.1 SICHERHEITSGRUNDSATZ.....	37
15.2 ADMINISTRATIVE ZUGRIFFE	37
15.3 ZUGRIFF DES AUFTRAGGEBERS.....	37
15.4 SECURITY INCIDENTS	37
15.5 DATENSCHUTZ UND VERTRAULICHKEIT	37
<u>16 MODERNISIERUNGS- UND INTEGRATIONSLEISTUNGEN</u>	38

16.1 GRUNDSATZ.....	38
16.2 INTEGRATIONSPROZESS.....	38
16.3 ZIELBILD- UND UMSETZUNGSKONZEPT.....	38
16.4 PARALLEL BETRIEB CMO/FMO	39
16.5 ABHÄNGIGKEITEN UND MITWIRKUNGEN.....	39
16.6 TMO – ÜBEFÜHRUNG VOM LEGACY-LAN IN DAS ZIELBETRIEBSMODELL	39
16.6.1 GROBPLANUNG UND HIGH-LEVEL-DESIGN	40
16.6.2 SYSTEM DESIGN / LOW-LEVEL-DESIGN	40
16.6.3 VORBEREITUNG PILOT / TECHNISCHE VALIDIERUNG	40
16.6.4 PoC / TECHNISCHE VALIDIERUNG	41
16.6.5 MIGRATION PLAN / ROLLOUT-PLANUNG UND RUNBOOK	41
16.6.6 PARALLELER PILOTBETRIEB	41
16.6.7 ROLLOUT UND MIGRATION IN DEN ZIELBETRIEB	41
16.6.8 WORKSHOPS UND KNOW-HOW-TRANSFER	42
16.6.9 DOKUMENTATION UND BETRIEBSÜBERNAHME.....	42
16.6.10 PROJEKTMANAGEMENT DER TMO-LEISTUNGEN	42
16.6.11 RISIKO- UND PUFFERPOSITION	43
 <u>17 LIFECYCLE-, EOL-/EOS- UND RMA-MANAGEMENT</u>	 <u>44</u>
17.1 LIFECYCLE-MANAGEMENT	44
17.2 EOL-/EOS-REGISTER	44
17.3 RMA-ROLLE DES AUFTRAGNEHMERS.....	44
17.4 SPARES- UND ERSATZTEILKONZEPT	44
17.5 UMGANG MIT NICHT SUPPORTETEN KOMPONENTEN	44
17.6 HERSTELLERBEZOGENER SOFTWARE-SUPPORT, BUGFIXES UND UPDATES	45
 <u>18 SERVICE LEVEL, ESKALATION UND QUALITÄTSSICHERUNG.....</u>	 <u>46</u>
18.1 SERVICEZEITEN	46
18.2 SLA-MODELL	46
18.3 ESKALATIONSMATRIX.....	46
18.4 QUALITÄTSSICHERUNG	46
18.5 ENTSCHULDBARE LEISTUNGSMINDERUNGEN	46
18.6 MALUS-REGELUNG BEI SLA-VERLETZUNGEN	46
18.7 MALUS BEI VERLETZUNG VON INCIDENT-SLAS.....	47
18.8 MALUS BEI WIEDERHOLTEN VERFÜGBARKEITSVERLETZUNGEN	47
18.9 MALUS BEI PROZESS- UND DOKUMENTATIONSVERLETZUNGEN	47
18.10 REPORTING UND MESSUNG.....	48
18.11 DECKELUNG DER MALUS-BETRÄGE	48
 <u>19 BETRIEBSORGANISATION, ROLLEN UND GOVERNANCE.....</u>	 <u>49</u>
19.1 ROLLEN DES AUFTRAGNEHMERS	49
19.2 QUALIFIKATIONSANFORDERUNGEN	49
19.3 MEETINGSTRUKTUR	49
19.4 RESSOURCEN- UND FLUKTUATIONSMANAGEMENT	49

20 KALKULATIONS- UND ABRECHNUNGSMODELL	50
20.1 GRUNDSATZ.....	50
20.2 PREISBESTANDTEILE	50
20.3 PORT-KATEGORIEN	52
20.4 CMO-/FMO-ABGRENZUNG	52
20.5 ABGRENZUNG ZWISCHEN LAUFENDEM BETRIEB UND ÜBERFÜHRUNG IN DAS ZIELBETRIEBSMODELL	53
20.6 ZUORDNUNG DER PORT-PAUSCHALE ZU DEN MANAGED-SERVICE-LEISTUNGEN	53
20.7 ZÄHL- UND ABRECHNUNGSREGELN	54
21 ANFORDERUNGEN AN EINZUREICHENDE KONZEPTE.....	54
21.1 PROJEKT-, TRANSITION- UND BETRIEBSÜBERNAHMEKONZEPT	54
21.2 MANAGED-SERVICE- UND BETRIEBSKONZEPT	55
21.3 ZIELBILD-, STANDARDISIERUNGS- UND AUTOMATISIERUNGSKONZEPT	55
21.4 LIFECYCLE- UND RISIKOMANAGEMENTKONZEPT	55
21.5 EXIT- UND PROVIDERWECHSELKONZEPT	55
22 ABNAHMEN, NACHWEISE UND VERTRAGSSTEUERUNG.....	56
22.1 ABNAHMEARTEN.....	56
22.2 NACHWEISPFlichten.....	56
22.3 VERTRAGSSTEUERUNG	56
23 EXIT MANAGEMENT	57
23.1 ZIEL	57
23.2 LAUFENDE EXIT-FÄHIGKEIT	57
23.3 FORMALE EXIT-PHASE	57
23.4 ÜBERGABEOBJEKTE	57
23.5 UNTERSTÜTZUNG DES NACHFOLGEPROVIDERS.....	57
23.6 RÜCKGABE UND LÖSCHUNG.....	57

Tabellenverzeichnis

Tabelle 1: Abkürzungsverzeichnis.....	7
Tabelle 2: Leistungsumfang im Scope	9
Tabelle 3: Betriebsphasen und Zielmodell	10
Tabelle 4: Schnittstellenverantwortung	13
Tabelle 5: Netzwerkkomponenten UKF-Bestand	16
Tabelle 6: Netzwerkkomponenten Sachsenhausen	17
Tabelle 7: EoS-relevante Komponenten UKF	17
Tabelle 8: EoS-relevante Komponenten Sachsenhausen	17
Tabelle 9: Automatisierungsfelder	19
Tabelle 10: Cisco-Kompetenzanforderungen	20
Tabelle 11: SOT-Arbeitspakete	21
Tabelle 12: SOT-Informationsarten	22
Tabelle 13: SOT-Ergebnisdokumente	22
Tabelle 14: Service-Request-Klassen	24
Tabelle 15: Mindestinhalt Ticketinformation	26
Tabelle 16: Monitoring-Metriken	27
Tabelle 17: Incident-Prioritäten und SLA.....	29
Tabelle 18: Problem-Kategorien.....	31
Tabelle 19: UKF-Verfahrensarten und Change-Typen	32
Tabelle 20: Betriebs-KPIs.....	33
Tabelle 21: CMDB-Pflichtinformationen	34
Tabelle 22: Konfigurationssicherung Schritte	37
Tabelle 23: CMDB-Datenfelder	39
Tabelle 24: Servicezeiten	40
Tabelle 25: Eskalationsmatrix.....	40
Tabelle 26: Rollen des Auftragnehmers	41
Tabelle 27: Meetingstruktur	41
Tabelle 28: Preisbestandteile	43

Abkürzungsverzeichnis

Abkürzung	Bedeutung
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AN	Auftragnehmer
AP	Access Point
CAB	Change Advisory Board
CI	Configuration Item
CMDB	Configuration Management Database
CMO	Current Mode of Operation, aktueller Betriebsmodus der bestehenden Infrastruktur
EoL	End of Life
EoS	End of Support
FMO	Future Mode of Operation, Zielbetriebsmodus
HA	High Availability
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
KEDB	Known Error Database
KRITIS	Kritische Infrastruktur
LAN	Local Area Network
MAB	MAC Authentication Bypass
NAC	Network Access Control
NOC	Network Operation Center
RCA	Root Cause Analysis
RMA	Return Material Authorization
SLA	Service Level Agreement
SOC	Security Operation Center
SOT	Service Ownership Transfer
TACACS+	Terminal Access Controller Access-Control System Plus
TTS	Trouble Ticket System
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
WLAN	Wireless Local Area Network

Tabelle 1: Abkürzungsverzeichnis

1 Präambel und Leistungsgegenstand

1.1 Ausgangssituation

Das Universitätsklinikum Frankfurt betreibt eine historisch gewachsene und für den Klinikbetrieb geschäftskritische LAN- und WLAN-Infrastruktur. Die bestehende aktive Netzwerkinfrastruktur basiert im Wesentlichen auf Cisco-Komponenten. Diese Infrastruktur ist Grundlage für medizinische, administrative, technische und versorgungsrelevante Anwendungen des Auftraggebers.

Der Betrieb dieser Infrastruktur muss auch während des Übergangs in einen neu ausgeschrieben Managed Service stabil, nachvollziehbar und mit klaren Verantwortlichkeiten erfolgen. Die Leistung richtet sich daher nicht nur auf eine reaktive Störungsbearbeitung, sondern auf einen ganzheitlichen Netzwerkbetrieb mit Monitoring, Serviceprozessen, Dokumentation, Lifecycle-Bewertung, Sicherheitsintegration und geordneter Weiterentwicklung der Betriebsarchitektur.

Der Schwerpunkt dieses Leistungsverzeichnisses liegt auf den Managed Services, der Betriebsübernahme, dem stabilen Betrieb der bestehenden Cisco-Infrastruktur und der Integration durch den Auftraggeber bereitgestellter oder separat beschaffter Komponenten.

1.2 Ziel der Ausschreibung

Ziel der Ausschreibung ist der Abschluss eines Vertrages über die Managed Services für die LAN- und WLAN-Infrastruktur des Auftraggebers. Der Auftragnehmer soll die bestehende Infrastruktur übernehmen, betreiben, stabilisieren und so weiterentwickeln, dass ein belastbarer, transparenter und dauerhaft steuerbarer Netzwerkbetrieb entsteht.

Die Leistung muss die Anforderungen eines Klinikums mit KRITIS-Bezug berücksichtigen. Der Auftragnehmer muss in der Lage sein, Ausfälle, Störungen, Änderungen und Sicherheitsereignisse unter Berücksichtigung klinischer Betriebsprozesse zu behandeln. Dazu gehören kurze Eskalationswege, belastbare Servicezeiten, strukturierte Dokumentation, klare Kommunikationswege und ein qualifiziertes technisches Team.

Ein wesentliches Ziel ist es, die Abhängigkeit von Einzelwissen und manuell geprägten Betriebsabläufen zu reduzieren. Der Auftragnehmer hat standardisierte Betriebsverfahren aufzubauen, bestehende Dokumentationen zu prüfen und fortzuschreiben sowie die Servicequalität messbar zu machen.

1.3 Leistungsgegenstand

Gegenstand dieses Leistungsverzeichnisses sind alle Leistungen, die für die Übernahme, Fortführung, Steuerung und Weiterentwicklung des LAN-/WLAN-Betriebs erforderlich sind. Der Auftragnehmer übernimmt die operative Verantwortung für die im Scope befindlichen Netzwerkkomponenten und Betriebsprozesse.

Zum Leistungsgegenstand gehören insbesondere die Betriebsübernahme, der laufenden Managed Services, Incident-, Problem-, Change-, Release- und Configuration-Management, Monitoring, Reporting, Dokumentation, Lifecycle-Management, Unterstützung bei EoL-/EoS-Risiken, Unterstützung bei RMA- und Herstellerprozessen sowie Integrationsleistungen für bereitgestellte oder separat beschaffte Komponenten.

Nicht Gegenstand der regulären Leistung ist die Lieferung der aktiven Netzwerkhardware. Soweit Hardware, Lizenzen oder Herstellerwartung benötigt werden, erfolgt die Beschaffung grundsätzlich über den Auftraggeber oder über gesonderte Beschaffungswege. Der Auftragnehmer hat jedoch die Fähigkeit nachzuweisen, diese Komponenten technisch zu bewerten, in den Betrieb zu übernehmen und in die Serviceprozesse zu integrieren.

Leistungsbereich	Im Scope
Managed Service LAN/WLAN	Betrieb, Monitoring, Incident, Problem, Change, Release, Reporting
Cisco-Bestandsbetrieb	Betrieb und Entstörung der bestehenden Cisco-Infrastruktur
Hardware	Bewertung, Integration, Konfiguration und Betriebsübernahme bereitgestellter Komponenten
Lifecycle	EoL-/EoS-Bewertung, Risikomeldung, Handlungsempfehlung
Modernisierung	Konzept, Integration, Test, Abnahmeunterstützung, Betriebsüberführung

Leistungsbereich	Im Scope
Exit	Übergabe, Dokumentation, Datenexport, Knowledge Transfer

Tabelle 2: Leistungsumfang im Scope

1.4 Verbindliche Kompetenzanforderung für Cisco-Bestandsbetrieb

Da die bestehende Infrastruktur im Wesentlichen auf Cisco-Komponenten basiert, muss der Bieter nachweisen, dass er den Betrieb einer Cisco-basierten Enterprise-LAN-/WLAN-Umgebung fachlich, organisatorisch und personell beherrscht. Dies betrifft insbesondere Switching, Routing, WLAN-Controller, Access Points, Managementsysteme, Konfigurationssicherung, Troubleshooting, Firmware-/Release-Bewertung und Herstellerfallbearbeitung.

Der Bieter muss geeignetes Personal mit praktischer Erfahrung im Betrieb vergleichbarer Cisco-Infrastrukturen bereitstellen. Dazu gehören mindestens Ressourcen für Architektur, Betrieb, 2nd-/3rd-Level-Support, Change-/Release-Bewertung und Eskalation. Die entsprechenden Rollen, Qualifikationen und Vertretungen sind im Angebot darzustellen und während der Vertragslaufzeit aufrechtzuerhalten.

Diese Kompetenzanforderung ist für die sichere Betriebsübernahme und den CMO-Betrieb zwingend erforderlich. Der Auftraggeber erwartet, dass der Auftragnehmer die bestehende Cisco-Infrastruktur ohne längere Einarbeitungsrisiken übernehmen und betreiben kann.

1.5 Grundsätze der Leistungserbringung

- Der Klinikbetrieb darf durch Betriebsübernahme, Störungsbearbeitung, Changes oder Integrationsleistungen nicht vermeidbar beeinträchtigt werden.
- Der Auftragnehmer arbeitet nach dokumentierten, nachvollziehbaren und freigegebenen Prozessen.
- ServiceNow des Auftraggebers ist das führende System für Tickets, Status, Nachweise und Eskalationen.
- Der Auftragnehmer ist für die Pflege der betriebsrelevanten Dokumentation verantwortlich.
- Alle administrativen Zugriffe müssen personalisiert, abgesichert und protokolliert erfolgen.
- EoL-/EoS- und Lifecycle-Risiken sind aktiv zu bewerten und regelmäßig zu berichten.
- Die Providerwechselfähigkeit ist während der gesamten Vertragslaufzeit sicherzustellen.

2 Betriebsphasen und Zielmodell

2.1 Phasenübersicht

Die Leistung ist in mehrere Betriebs- und Projektphasen gegliedert. Diese Phasen bilden die Grundlage für Aufgaben, Verantwortlichkeiten, Abnahmen, Service Levels und Vergütung. Ziel ist, die bisherigen Unschärfen zwischen Übernahme, Regelbetrieb, Modernisierung und Zielbetrieb zu vermeiden.

Der Auftragnehmer muss die Phasen im Angebot in einem Projekt- und Betriebsplan abbilden. Der Plan muss realistische Abhängigkeiten berücksichtigen, insbesondere die Verfügbarkeit von Dokumentation, Zugängen, Personal, passiver Infrastruktur, bereitgestellter Hardware und Freigaben des Auftraggebers.

Phase	Bezeichnung	Schwerpunkt	Verbindliches Ergebnis
1	Service Ownership Transfer (SOT)	Übernahmenvorbereitung, Due Diligence, Tool- und Prozessanbindung	Abnahmefähige Betriebsübernahme
2	Current Mode of Operation (CMO)	Betrieb der bestehenden Cisco-Infrastruktur	Stabiler Managed Service für den Bestand
3	Stabilisierung und Zielbildplanung	Bewertung des Bestands, Risikoanalyse, Zielbild und Integrationsplanung	Freigegebenes Zielbild- und Umsetzungskonzept
4	Integrations- und Modernisierungsphase	Integration bereitgestellter oder separat beschaffter Komponenten	Überführung definierter Netzbereiche in den Zielbetrieb
5	Future Mode of Operation (FMO)	Betrieb modernisierter Netzbereiche mit höherem Standardisierungsgrad	Messbarer Zielbetrieb
6	Exit / Providerwechsel	Geordnete Übergabe, Datenexport, Wissenstransfer	Übergabefähiger Service

Tabelle 3: Betriebsphasen und Zielmodell

2.2 Service Ownership Transfer (SOT)

Die SOT-Phase beginnt mit Zuschlag bzw. mit dem vertraglich festgelegten Starttermin. In dieser Phase übernimmt der Auftragnehmer schrittweise die fachliche, technische und organisatorische Verantwortung für den Betrieb. Die SOT-Phase dient nicht dazu, grundlegende Kalkulationsannahmen nachträglich zu verändern, sondern dazu, die übergebenen Informationen zu prüfen, den Betrieb einzurichten und Lücken transparent zu machen.

Während der SOT-Phase muss der Auftragnehmer parallel zur Dokumentationsprüfung bereits die Voraussetzungen für den späteren Regelbetrieb schaffen. Hierzu zählen der Aufbau sicherer Zugänge, die Einbindung in ServiceNow, die Anbindung oder Nutzung vorhandener Monitoringinformationen, die Festlegung der Meldewege, die Erstellung einer Eskalationsmatrix und die Erarbeitung eines initialen Betriebshandbuchs.

Die SOT-Phase endet erst, wenn die im Kapitel zur Betriebsübernahme definierten Abnahmekriterien erfüllt sind. Vor diesem Zeitpunkt gelten SLA nur in dem Umfang, der für die Übergangsphase ausdrücklich vereinbart ist.

2.3 Current Mode of Operation (CMO)

Der CMO umfasst den Betrieb der bestehenden Cisco-basierten LAN-/WLAN-Infrastruktur. In dieser Phase liegt der Schwerpunkt auf Stabilität, Nachvollziehbarkeit, Störungsbearbeitung, Risikotransparenz und kontrollierten Changes.

Der Auftragnehmer muss die bestehende Infrastruktur betreiben, auch wenn einzelne Komponenten abgekündigt sind oder nur eingeschränkt durch den Hersteller unterstützt werden. Soweit technische Einschränkungen bestehen, sind diese unverzüglich zu melden, zu bewerten und mit Maßnahmenvorschlägen zu hinterlegen. Der Auftragnehmer darf Einschränkungen nicht erst im Störfall geltend machen, wenn diese bei ordnungsgemäßer Lifecycle-Prüfung vorher erkennbar gewesen wären.

Der CMO ist nicht als reiner Übergangsnottbetrieb zu verstehen. Er ist ein vollwertiger Managed Service für den vorhandenen Bestand, solange dieser Bestand produktiv betrieben wird.

2.4 Stabilisierung und Zielbildplanung

Nach der Betriebsübernahme muss der Auftragnehmer die Umgebung stabilisieren und die Weiterentwicklung des Betriebs fachlich strukturieren. Die Stabilisierung beinhaltet die Prüfung wiederkehrender Störungen, die Bewertung von Schwachstellen, die Konsolidierung der Dokumentation und die Festlegung von betrieblichen Standards.

Parallel dazu erstellt der Auftragnehmer ein Zielbild- und Umsetzungskonzept. Dieses Konzept beschreibt nicht die Beschaffung konkreter Hardware, sondern den Weg zu einem besseren Betriebsmodell. Es muss zeigen, wie Standardisierung, Automatisierung, Segmentierung, Monitoring und Providerwechselfähigkeit verbessert werden können.

Das Zielbildkonzept muss so konkret sein, dass es als Grundlage für spätere Integrationsmaßnahmen und für separate Hardwarebeschaffungen verwendet werden kann. Es muss Abhängigkeiten, Risiken, Reihenfolgen, Meilensteine und Abnahmekriterien enthalten.

2.5 Integrations- und Modernisierungsphase

Die Integrations- und Modernisierungsphase beginnt, sobald der Auftraggeber Komponenten bereitstellt oder über separate Beschaffungswege Komponenten verfügbar macht, die in den Managed Service übernommen werden sollen. Der Auftragnehmer unterstützt in dieser Phase Planung, Vorbereitung, Konfiguration, Inbetriebnahme, Test, Dokumentation und Betriebsüberführung.

Der Auftragnehmer ist nicht Lieferant der Hardware, sofern dies nicht ausdrücklich als separate Leistung beauftragt wird. Er ist jedoch verantwortlich dafür, die Übernahmefähigkeit zu prüfen, technische Risiken zu melden und die Komponenten nach erfolgreicher Abnahme in den Betrieb zu integrieren.

Die bisherige Vorstellung einer starren FMO-Light-Phase mit vollständig hausweisem Hardwaretausch wird durch ein flexibles, aber verbindlich gesteuertes Integrationsmodell ersetzt. Damit können passive Abhängigkeiten, Budget- und Beschaffungszeitpunkte sowie betriebliche Prioritäten realistisch berücksichtigt werden.

2.6 Future Mode of Operation (FMO)

Der FMO beschreibt den Zielbetrieb modernisierter oder standardisierter Netzbereiche. Gegenüber dem CMO muss der FMO durch höhere Transparenz, bessere Dokumentation, konsistentere Betriebsverfahren, stärkere Automatisierung und bessere Messbarkeit gekennzeichnet sein.

Ein Netzbereich wird erst dann dem FMO zugeordnet, wenn die definierten Übernahmekriterien erfüllt sind. Dazu gehören erfolgreiche technische Tests, Monitoringanbindung, CMDB-Pflege, Konfigurationssicherung, aktualisierte Dokumentation und formale Abnahme durch den Auftraggeber.

Der Auftragnehmer muss CMO- und FMO-Bereiche während der Vertragslaufzeit parallel betreiben können. Die jeweiligen Servicequalitäten, Verantwortlichkeiten und Abrechnungsgrundlagen sind transparent auszuweisen.

2.7 Exit-Phase

Die Exit-Phase umfasst die geordnete Übergabe aller Leistungen, Dokumentationen und Betriebsdaten an den Auftraggeber oder einen Nachfolge-Auftragnehmer. Providerwechselfähigkeit ist von Beginn an sicherzustellen. Die Einzelheiten regelt Kapitel 23.

3 Leistungsumfang, Scope und Abgrenzung

3.1 Im Scope befindliche Leistungen

Der Leistungsumfang umfasst alle Tätigkeiten, die für einen sicheren und steuerbaren Betrieb der LAN-/WLAN-Infrastruktur erforderlich sind. Die Leistungen sind als Managed Service zu verstehen und nicht als einzelvorgangsbezogene Unterstützung ohne Gesamtverantwortung.

Die im Scope befindlichen Komponenten werden im Rahmen der SOT-Phase final verifiziert. Der Auftraggeber stellt hierfür vorhandene Assetinformationen, Netzpläne, Port- und Standortinformationen sowie vorhandene Betriebsdokumentationen bereit. Der Auftragnehmer ist verpflichtet, diese Informationen zu prüfen und Abweichungen strukturiert zu dokumentieren.

- Managed Service für LAN-Komponenten im Core-, Distribution- und Access-Bereich.
- Managed Service für WLAN-Controller, Access Points und zugehörige Managementkomponenten.
- Betrieb bestehender Cisco-Komponenten einschließlich qualifiziertem 2nd-/3rd-Level-Support.
- Monitoring, Eventbewertung, Incidentbearbeitung und Eskalation.
- Problem Management inklusive Ursachenanalyse und Known-Error-Pflege.
- Change- und Release-Management für produktive Netzwerkänderungen.
- Konfigurationssicherung und Wiederherstellung.
- CMDB-/Asset-Pflege für betreute Komponenten.
- Lifecycle-, EoL-/EoS- und Risiko-Reporting.
- Integrationsleistungen für durch UKF bereitgestellte oder separat beschaffte Komponenten.
- Dokumentation, Betriebshandbuch und Knowledge Management.
- Exit- und Providerwechselunterstützung.

3.2 Nicht im regulären Scope befindliche Leistungen

Zur Vermeidung von Fehlinterpretationen werden die nicht im regulären Scope befindlichen Leistungen ausdrücklich abgegrenzt. Diese Abgrenzung ist wesentlich für Kalkulation, Preismatrix und Risikoverteilung.

- Regelmäßige Lieferung aktiver Netzwerkkomponenten durch den Auftragnehmer.
- Finanzierung oder Lagerhaltung eines vollständigen Hardware-Zielbestands durch den Auftragnehmer.

3.3 Schnittstellen zu separaten Hardwarebeschaffungen

Der Auftragnehmer unterstützt die Integration von aktiver Netzwerkhardware auch dann, wenn diese separat beigestellt oder aus Lagerbeständen entnommen wird. Die Voraussetzung hierfür ist, dass der Auftraggeber die hierzu benötigten technischen Informationen rechtzeitig zur Verfügung stellt.

Der Auftragnehmer muss die Übernahmefähigkeit der Komponenten prüfen und etwaige Bedenken vor Inbetriebnahme anzeigen. Bedenken können sich aus fehlender Herstellerunterstützung, fehlenden Lizenzen, inkompatiblen Softwareständen, nicht erfüllten Sicherheitsanforderungen, fehlenden Schnittstellen oder unvollständiger Dokumentation ergeben.

Schnittstelle	Verantwortung Auftraggeber	Verantwortung Auftragnehmer
Hardwarebeschaffung	Beschaffung, Lieferung, Lizenzierung und Wartungsgrundlagen	Benennung betrieblicher Mindestvoraussetzungen und Bedenkenanzeige
Bereitstellung	Lieferzeitpunkt, Seriennummern, Standort, Eigentums- und Lizenznachweise	Prüfung der Übernahmefähigkeit
Integration	Freigaben, Wartungsfenster, Drittkoordination	Planung, Konfiguration, Test, Dokumentation
Betriebsübernahme	Abnahmeentscheidung und Mitwirkung	Monitoring, CMDB, Betriebshandbuch, Konfigurationssicherung
RMA	Bereitstellung von Wartungsvertrag oder Ersatzhardware	Diagnose, Koordination, Wiederinbetriebnahme, Dokumentation

Tabelle 4: Schnittstellenverantwortung

3.4 Standort- und Scope-Erweiterungen

Der Managed Service muss so ausgestaltet sein, dass zusätzliche Standorte, Gebäude, Funktionsbereiche oder organisatorisch zugeordnete Einheiten des Auftraggebers in den Scope aufgenommen werden können. Dies gilt insbesondere für Netzbereiche, die während des Verfahrens oder während der Vertragslaufzeit zusätzlich in den Verantwortungsbereich des Auftraggebers fallen. Der Bestand Sachsenhausen ist als gesonderter, zeitversetzt einzubeziehender Scope auszuweisen. Er wird nicht Bestandteil des initialen CMO-Betriebs des UKF-Campus Frankfurt, sondern planmäßig nach Ablauf von 24 Monaten ab Leistungsbeginn in den Managed Service überführt. Die laufende Servicevergütung, SLA-Wirksamkeit und Mengenberücksichtigung für Sachsenhausen beginnen erst mit der formalen Aufnahme in den Leistungsumfang. Die Abbildung erfolgt in der Preismatrix über einen separaten Mengen- und Wertungsansatz für Sachsenhausen ab Monat 25.

Der Managed Service muss so ausgestaltet sein, dass während der Vertragslaufzeit auch größere Erweiterungen der WLAN-Infrastruktur in den Leistungsumfang aufgenommen werden können. Dies umfasst insbesondere die Integration, Konfiguration, Dokumentation, Monitoringanbindung, CMDB-Pflege und formale Betriebsübernahme zusätzlicher durch den Auftraggeber bereitgestellter oder separat beschaffter WLAN-Access-Points.

Die Lieferung der Access-Point-Hardware ist hiervon nicht umfasst, sofern sie nicht ausdrücklich gesondert beauftragt wird. Die kalkulatorische Abbildung definierter WLAN-Erweiterungsszenarien erfolgt im Kalkulations- und Abrechnungsmodell sowie in der Preismatrix.

Der Auftragnehmer muss hierfür ein standardisiertes Verfahren zur Scope-Erweiterung vorsehen. Dieses Verfahren umfasst Bestandsaufnahme, Risikoprüfung, Aufwandsschätzung, Integration, Dokumentation, CMDB-Pflege und formale Betriebsübernahme.

4 Technische Systemlandschaft - IST-Zustand

4.1 Gesamtüberblick

Die aktuelle LAN-/WLAN-Infrastruktur des Auftraggebers basiert überwiegend auf Cisco-Technologie und ist historisch gewachsen. Sie umfasst zentrale Core-/Backbone-Komponenten, Gebäude- und Verteilerebenen, Access-Switches, WLAN-Controller, Access Points sowie ergänzende Management-, Monitoring-, NAC- und AAA-Komponenten.

Die Infrastruktur ist aktuell überwiegend durch eine Layer-2-geprägte Campusstruktur mit mehr als 400 VLANs gekennzeichnet. Das interne VLAN-Routing erfolgt überwiegend über zentrale Routing- und Sicherheitsinstanzen, insbesondere über Segmentierungsfirewalls und dedizierte zentrale Routing-Systeme. Eine vollständig einheitliche Trennung zwischen Access-, Distribution- und Core-Layer ist noch nicht in allen Bereichen erreicht.

Aufgrund der zentralen Routingarchitektur werden viele VLANs über größere Campusbereiche geführt. Daraus ergeben sich im Betrieb erhöhte Anforderungen an Change-Koordination, Fehleranalyse, Dokumentation und Segmentierungssteuerung. Redundante Pfade sind nicht in allen Bereichen vollständig umgesetzt; bei neueren Inbetriebnahmen werden redundante Anbindungen jedoch grundsätzlich berücksichtigt.

Der Auftragnehmer muss den IST-Zustand im Rahmen der SOT-Phase fachlich verifizieren. Abweichungen, fehlende Dokumentation, besondere Betriebsrisiken und Einschränkungen aus Lifecycle- oder Supportstatus sind im Due-Diligence-Bericht und im Betriebshandbuch zu dokumentieren.

4.2 Core- und Backbone-Bereich

Das Campusnetz verfügt über zwei zentrale Core-Standorte, das Hauptrechenzentrum und das Backup-Rechenzentrum. Beide Standorte sind über redundante Glasfaserverbindungen gekoppelt.

Im Bestand werden Cisco Nexus 9504-Systeme als zentrale Switching-Instanzen auf Backbone-Ebene eingesetzt. Das produktive Layer-3-Routing erfolgt nicht durchgängig auf den Nexus-Core-Systemen, sondern überwiegend über separate zentrale Routing- und Sicherheitsinstanzen. Im Bestand sind hierfür unter anderem Cisco Catalyst 9500-Systeme als Routing-Komponenten eingesetzt.

Dynamische Routing-Protokolle sind im Bestand nicht flächendeckend als einheitliches Campus-Betriebsmodell umgesetzt. Änderungen im Core-/Backbone-Bereich sind aufgrund der zentralen Wirkung grundsätzlich mit erhöhter Sorgfalt zu planen, zu testen, freizugeben und zu dokumentieren.

4.3 Topologie, Distribution und Access

Der Campus weist überwiegend eine dreistufige Struktur aus Access, Distribution und Core auf. In wenigen Ausnahmefällen bestehen direkte Anbindungen von Access-Komponenten an die Core-Systeme. In einzelnen größeren Versorgungseinheiten sind Cisco Catalyst 9407R als Aggregations- bzw. Distributionssysteme im Einsatz.

Im Access-Bereich werden unterschiedliche Cisco Catalyst-Generationen betrieben. Neben Catalyst 9200L, 9200CX, 9300 und 9300LM sind ältere Gerätegenerationen wie Catalyst 2960, 3560, 3750 und 3850 im Bestand vorhanden. Teilbereiche weisen dadurch unterschiedliche Softwarestände, Featureumfänge, PoE-Leistungsfähigkeiten und Lifecycle-Status auf.

In einzelnen Bereichen bestehen kaskadierte Access-Strukturen sowie ältere Inhouse-Verkabelungen mit besonderen Anschluss- oder Aufteilungsvarianten. Diese Besonderheiten sind im Rahmen der Betriebsübernahme zu verifizieren und in den Betriebsunterlagen kenntlich zu machen.

4.4 WLAN-Infrastruktur

Das bestehende WLAN basiert auf einer zentral gesteuerten Cisco-Controller-Architektur. Im Bestand befinden sich Access Points unterschiedlicher Generationen sowie WLAN-Controller der bestehenden Cisco-WLAN-Plattform.

Die WLAN-Abdeckung und Leistungsfähigkeit ist gebäude- und nutzungsabhängig unterschiedlich ausgeprägt. Ein zentrales RF-Management ist grundsätzlich vorhanden; die flächendeckende Nutzung wird durch Skalierungs- und Standortgrenzen der eingesetzten Managementplattform beeinflusst. Ein automatisiertes Leistungs- und Kanal-Tuning der WLAN-Infrastruktur ist implementiert.

Das WLAN-Management erfolgt zentral über die vorhandenen Cisco-Management- und Controlleroberflächen. Die WLAN-Controller und Access Points sind in bestehende Monitoring-Systeme wie PRTG und Cisco Catalyst Center eingebunden. Ergänzend wird Cisco Spaces für Analyse- und Erweiterungsfunktionen eingesetzt. Zusätzlich ist eine Hypros-Lösung mit BLE-Bezug im Bestand zu berücksichtigen.

Der Auftragnehmer muss WLAN-Störungen gesamtheitlich betrachten. Neben Funkparametern sind insbesondere Switching, PoE, Authentifizierung, DHCP/DNS, NAC, Controllerzustand, Roaming und Endgeräteverhalten in die Analyse einzubeziehen.

4.5 Verkabelung und passive Abhängigkeiten

Die aktive Infrastruktur ist über Glasfaserverbindungen auf Singlemode- und Multimode-Basis verbunden. Zwischen den zentralen Core-Standorten bestehen redundante Singlemode-Verbindungen. Innerhalb von Gebäuden sind weiterhin Multimode-Strecken vorhanden, auf denen nicht in allen Fällen die volle 10-Gbit/s-Übertragungsleistung erreicht wird.

Die Inhouse-Verkabelung ist abhängig von Bauabschnitt und Gebäude unterschiedlich ausgeführt. Eine vollständige Redundanz aller Leitungswege zwischen sämtlichen Verteilerschränken besteht nicht. Wesentliche Verteilerschränke sind jedoch in der Regel redundant an den jeweiligen Hauptverteiler angebunden.

Modernisierungs- und Integrationsmaßnahmen an aktiven Komponenten können von passiven Voraussetzungen wie Glasfaserverfügbarkeit, Verteilerstandorten, Stromversorgung, Trassen, Patchwegen oder baulichen Freigaben abhängen. Diese Abhängigkeiten sind im Rahmen der SOT und bei Integrationsmaßnahmen zu dokumentieren.

4.6 Betrieb, Management und Dokumentation

Für das Management der LAN- und WLAN-Infrastruktur wird Cisco Catalyst Center on-premises eingesetzt. Darüber werden nach derzeitigem Stand wesentliche Teile der Catalyst-basierten LAN- und WLAN-Infrastruktur zentral verwaltet. Das System unterstützt unter anderem Gerätemanagement, Konfigurationssicherung, Firmware-/Softwareverteilung, Inventarisierung und Grunddokumentation.

Das Catalyst Center wird regelmäßig gesichert. Die vorhandenen Funktionen werden jedoch nicht in allen Bereichen vollständig für End-to-End-Automatisierung, Template-Provisionierung, Orchestrierung oder durchgängige Prozessintegration genutzt.

Für das operative Monitoring ist PRTG als produktives Monitoring-System im Einsatz. Eine unternehmensweit vollständig gepflegte CMDB mit durchgängiger Verknüpfung von Assets, Services, Anwendungen, Changes und Abhängigkeiten ist im Bestand nicht vollständig etabliert.

Incident-, Problem- und Change-Prozesse sind organisatorisch vorhanden, jedoch nicht durchgängig Ende-zu-Ende technisch mit Netzwerk-, Asset- und Konfigurationsdaten integriert. Ein SOC/SIEM wird durch einen externen Dienstleister betrieben.

4.7 NAC, AAA und Security-Schnittstellen

Im Bereich Network Access Control und AAA sind mehrere Systeme mit getrennten Rollen im Einsatz. Cisco ISE wird im Bestand für TACACS+-basierte Authentifizierung, Autorisierung und Accounting der Netzwerkadministration genutzt.

Cisco ISE ist im Bestand nicht als RADIUS-Server für Endgeräte-NAC konfiguriert und liefert keine netzwerkbezogenen Endgeräte- oder Segmentierungsinformationen für den operativen Endgerätezugriff. Macmon NAC wird als RADIUS-basiertes NAC-System für Endgeräte-Authentifizierung eingesetzt.

Aufgrund der getrennten Einsatzszenarien besteht kein gemeinsames einheitliches Policy- oder Regelwerk zwischen Cisco ISE und macmon. Der Auftragnehmer muss diese Rollenverteilung im Betrieb berücksichtigen und im Betriebshandbuch dokumentieren.

4.8 Eingesetzte aktive Netzwerkkomponenten im UKF-Bestand

Die nachfolgende Übersicht beschreibt den zum Zeitpunkt der Erstellung bekannten aktiven Komponentenbestand des UKF-Campus Frankfurt. Die Angaben dienen der Einordnung des Betriebsumfangs, der erforderlichen Cisco-Betriebskompetenz und der Kalkulation des CMO-Managed-Service. Die aufgeführten Komponenten stellen keinen Hardware-Lieferumfang des Auftragnehmers dar.

Bereich	Komponente / Gerätefamilie	Menge UKF	Betriebliche Einordnung
Core / Backbone	Cisco Nexus 9504	4	zentrale Backbone-Switching-Systeme
Routing / Core-nah	Cisco Catalyst 9500, Modelle 12Q RTR-Klinet	2	zentrale Routing-/Sonderfunktion
Distribution / HVT	Cisco Catalyst 9500, Serien 16X, 40X, 24Y4C, 48Y4C	50	Distribution / Glasfaser- und Gebäudekopplung
Distribution / Aggregation	Cisco Catalyst 9407R	3	Aggregations- bzw. Distributionssysteme
Distribution / Aggregation	Cisco C9407R	4	Aggregations- bzw. Distributionssysteme
Compact / Sonderstandorte	Cisco C9200CX-8P-2X2G	4	kompakte Access-/Sonderkomponenten
Access	Cisco Catalyst 9200L	137	Access-Schicht
Access	Cisco Catalyst 9200CX / 9300 / 9300LM	336	Access-Schicht
Access Legacy	Cisco Catalyst 2960 / 3560 / 3750 / 3850	179	ältere Access-Komponenten
Office / Legacy Access	Cisco 2960 / 3560 Office-Switches	112	Office-/Sonderbestand
Legacy Aggregation	Cisco 2960 / 3560 / 3750 / 3850 / 4506 / 4500 / 6509	20	ältere Aggregationskomponenten
ToR / Rechenzentrumsumfeld	Cisco Nexus 9000 C93180YC-EX	8	ToR-Switches
FEX / Serveranbindung	Cisco Nexus N2K-C2348TQ-10G-E	84	Fabric Extender / betriebsrelevante Serveranbindung
WLAN	Cisco Access Points C9115AXI/AXE, C9120AXE, CW9164, CW9166	1.020	aktuelle WLAN-Infrastruktur
WLAN Controller	Cisco C9800-40 und CW9800M	4	zentrale WLAN-Controller
WLAN Legacy	Cisco Access Points der Serien 2602 und 3702	209	ältere WLAN-Infrastruktur
WLAN Controller Legacy	Cisco AIR-CT5520 und AIR-CT5508	2	ältere WLAN-Controller
Management	Cisco Catalyst Center Gen 2 Appliance	3	zentrales Netzwerkmanagement

Tabelle 5: Netzwerkkomponenten UKF-Bestand

Die Summe der switch- und FEX-relevanten Komponenten des UKF-Bestands beträgt auf Basis der vorliegenden Arbeitsdaten ca. 943 Komponenten. WLAN-Access-Points, WLAN-Controller, Management-Appliances, Module, Linecards, Supervisoren, Transceiver, Netzteile und reine Lizenzpositionen sind in dieser Switch-/FEX-Summe nicht enthalten, bleiben jedoch für den Managed Service betriebsrelevant.

4.9 Später einzubeziehender Bestand Sachsenhausen

Der Standort bzw. Bestand Sachsenhausen ist getrennt vom aktuellen UKF-Campusbestand auszuweisen. Die nachfolgend aufgeführten Komponenten sind als später in den Managed Service einzubeziehender Bestand zu verstehen. Sachsenhausen wird planmäßig nach Ablauf von 24 Monaten ab Leistungsbeginn, somit ab Monat 25, in den laufenden Managed Service überführt. Bis zu diesem Zeitpunkt sind die Komponenten nicht Bestandteil der initialen SLA-wirksamen CMO-Servicevergütung des UKF-Campus Frankfurt.

Bereich	Komponente / Gerätefamilie	Menge Sachsenhausen
Access	Cisco Catalyst 2960X	45
Compact / Mini-Switches	Cisco C9200CX-8P-2X2G-E	20
Distribution / Glasfaser	Cisco Catalyst 4500X	6
ToR / Rechenzentrumsumfeld	Cisco Nexus N9K-C93180YC-FX3	6
FEX / Serveranbindung	Cisco Nexus N2K-C2232PP	3
Nexus Switching	Cisco Nexus N3K-C3548P-XL	9
Nexus Switching	Cisco Nexus N5K-C5548UP	1
Legacy Aggregation / Core-nah	Cisco Catalyst C6506-E	1

Bereich	Komponente / Gerätefamilie	Menge Sachsenhausen
WLAN	Cisco AIR-AP2802I-E-K9	111
WLAN Legacy	Cisco AIR-CAP2602I-E-K9	2
WLAN Controller	Cisco AIR-CT5520-K9	2
AAA / NAC-nahe Komponente	Cisco ISE-VM-K9	2

Tabelle 6: Netzwerkkomponenten Sachsenhausen

Die Summe der switch- und FEX-relevanten Komponenten Sachsenhausen beträgt auf Basis der vorliegenden Assetdaten ca. 91 Komponenten. Diese Menge ist nicht mit dem initialen UKF-CMO-Bestand zu vermischen. Sie ist in der Preismatrix gesondert als später einsetzender Leistungsumfang abzubilden und erst ab Monat 25 bzw. ab formaler Betriebsübernahme von Sachsenhausen für Service, SLA und Abrechnung zu berücksichtigen. Vorbereitende Tätigkeiten, Abstimmungen oder Due-Diligence-Leistungen vor Monat 25 sind nur insoweit geschuldet, wie sie im Leistungsumfang und in der Preismatrix ausdrücklich vorgesehen sind.

4.10 Lifecycle- und EoS-relevante Komponenten

Die nachfolgenden Lifecycle-Informationen dienen der Risikoeinordnung im CMO-Betrieb. Der Auftragnehmer muss diese Informationen im Rahmen der SOT-Phase verifizieren, in ein EoL-/EoS-Register überführen und mindestens quartalsweise aktualisieren. Aus der Tabelle entsteht keine Verpflichtung des Auftragnehmers zur Lieferung von Ersatzhardware.

4.10.1 UKF-Campus Frankfurt

Komponente	Menge UKF	End of Service	Ersatz-/Zielprodukt laut Arbeitsstand
C3560G Kupferswitch	55	31.01.2018	C9300L / C9300LM
C3850 Kupferswitch	12	31.10.2025	C9300L / C9300LM
C3750 Kupferswitch	10	31.01.2018	C9300L / C9300LM
C2960X Kupferswitch	40	31.10.2027	C9300L / C9300LM
C3560CX MiniSwitch	100	30.04.2029	C9200CX
C4500X Glasfaserswitch	6	31.10.2025	C9500-48Y4C
C9500-40X Glasfaserswitch	12	30.04.2029	C9500-48Y4C
C9500-16X Glasfaserswitch	30	30.04.2031	C9500-48Y4C / C9500-24Y4C
C9500-12Q Kinet/Winet Router	4	30.04.2029	C9500-32QC
C2911 VPN Router	2	31.12.2022	Catalyst 8300-1N1S-6T
C3925 Voice Router	2	31.12.2022	Catalyst 8300-1N1S-6T
Catalyst Center Gen 2 Appliance	3	31.03.2029	Catalyst Center Appliance Gen 3
Aironet 2800 Access Point	620	31.10.2027	Catalyst 9164 Access Point
Aironet 2602I Access Point	125	31.12.2021	Catalyst 9164 Access Point
Nexus 9500 Linecard N9K-X9732C-EX	4	30.04.2028	N9K-X9736C-FX
C9407 Supervisor 1-XL	6	30.04.2030	C9400X-SUP-2XL
N9K-C93180YC-EX	8	31.08.2027	N9K-C93180YC-FX3

Tabelle 7: EoS-relevante Komponenten UKF

4.10.2 Sachsenhausen

Komponente	Menge Sachsenhausen	End of Service	Ersatz-/Zielprodukt laut Arbeitsstand
Cisco Catalyst 2960X	45	31.10.2027	C9300L / C9300LM
Cisco Catalyst 4500X	6	31.10.2025	C9500-48Y4C
Cisco Nexus N2K-C2232PP	3	30.09.2025	gemäß Zielarchitektur zu bewerten
Cisco Nexus N5K-C5548UP	1	31.05.2024	gemäß Zielarchitektur zu bewerten
Cisco Catalyst C6506-E	1	31.10.2025	gemäß Zielarchitektur zu bewerten
Cisco AIR-CT5520-K9	2	31.01.2027	gemäß WLAN-Zielarchitektur zu bewerten
Cisco AIR-AP2802I-E-K9	111	31.10.2027	Catalyst 9164 Access Point
Cisco AIR-CAP2602I-E-K9	2	31.12.2021	Catalyst 9164 Access Point

Tabelle 8: EoS-relevante Komponenten Sachsenhausen

Komponenten ohne hinterlegtes oder verifiziertes End-of-Service-Datum sind im Rahmen der Due Diligence zu prüfen. Dies gilt insbesondere für Komponenten, deren Modellinformationen in der Assetliste nur über Monitoring- oder Hostname-Informationen abgeleitet wurden.

4.11 Hinweis zur Bereitstellung detaillierter Asset-Informationen

Die vollständige und standortbezogene Assetliste der im Betrieb befindlichen aktiven Netzwerkkomponenten liegt beim Auftraggeber vor. Sie wird aus Gründen der Informationssicherheit nicht vollständig als frei zugänglicher Bestandteil der Vergabeunterlagen veröffentlicht.

Die detaillierte Assetliste wird den zugelassenen Bietern im weiteren Verfahren bzw. nach Unterzeichnung einer Vertraulichkeitsvereinbarung zur Verfügung gestellt. Die im Leistungsverzeichnis dargestellten Mengen und Komponenten dienen der technischen Einordnung, der Bewertung des Betriebsumfangs und der Kalkulation des CMO-Managed-Service.

Abweichungen, Ergänzungen oder Aktualisierungen, die im Rahmen der Due-Diligence-Phase festgestellt werden, sind durch den Auftragnehmer zu dokumentieren, in die CMDB zu überführen und im Betriebshandbuch nachzuführen.

Die im weiteren Verfahren bereitzustellenden Assetinformationen können auch Seriennummern, Lizenzstände, Supportlaufzeiten und vorhandene Herstellervertragsinformationen umfassen. Die Bereitstellung erfolgt nur an zugelassene Bieter und, soweit erforderlich, nach Unterzeichnung einer Vertraulichkeitsvereinbarung.

5 Zielbild des Managed-Service-Betriebs

5.1 Betriebszielbild

Das Zielbild des Managed Service ist ein stabiler, nachvollziehbarer und steuerbarer Netzwerkbetrieb. Der Auftragnehmer soll nicht lediglich auf Störungen reagieren, sondern einen strukturierten Betrieb mit messbarer Qualität sicherstellen.

Das Zielbild orientiert sich an den betrieblichen Anforderungen des Auftraggebers: hohe Verfügbarkeit, sichere administrative Prozesse, klare Rollen, aktuelle Dokumentation, transparente Serviceberichte, reproduzierbare Änderungen und aktive Risikosteuerung.

Die bestehende Cisco-Infrastruktur ist als Ausgangsbasis zu betreiben. Die zukünftige technische Entwicklung erfolgt auf Grundlage der durch den Auftraggeber bereitgestellten oder separat beschafften Komponenten und der mit dem Auftraggeber abgestimmten Zielarchitektur.

5.2 Zielbild für Standardisierung

Ein wesentlicher Schwachpunkt historisch gewachsener Netzwerke liegt in Sonderkonfigurationen, uneinheitlichen Betriebsweisen und schwer nachvollziehbaren Abhängigkeiten. Der Auftragnehmer muss daher eine Standardisierung des Betriebs aktiv vorantreiben.

Standardisierung bedeutet nicht, alle Netzbereiche technisch identisch zu machen. Sie bedeutet, dass gleichartige Anforderungen gleichartig umgesetzt, dokumentiert, überwacht und geändert werden. Abweichungen müssen begründet, freigegeben und dokumentiert sein.

- Einheitliche Namenskonventionen für Netzwerkkomponenten, Standorte, VLANs, Rollen und Betriebsobjekte.
- Standardisierte Portprofile für typische Anschlussarten.
- Standardisierte Change-Klassen und Change-Templates.
- Standardisierte Monitoringklassen und Alarmierungslogiken.
- Standardisierte Dokumentationsstruktur im Betriebshandbuch.
- Standardisierte Verfahren für Konfigurationssicherung und Restore.

5.3 Zielbild für Automatisierung

Automatisierung soll den Betrieb reproduzierbarer und weniger fehleranfällig machen. Der Auftragnehmer muss im Angebot darstellen, welche Betriebsaufgaben automatisiert, teilautomatisiert oder bewusst manuell mit Freigabeprozess durchgeführt werden.

Automatisierung darf nicht zu unkontrollierten Änderungen im Kliniknetz führen. Produktive Änderungen müssen nachvollziehbar, freigegeben, dokumentiert und rückrollbar sein. Automatisierung ist daher immer mit Change Management, Logging und Qualitätssicherung zu verbinden.

Automatisierungsfeld	Erwartung
Konfigurationssicherung	Regelmäßige automatische Sicherung und Vergleichbarkeit von Konfigurationsständen
Firmware-Compliance	Übersicht über freigegebene, installierte und abweichende Softwarestände
Portbereitstellung	Nutzung standardisierter Profile und dokumentierter Freigaben
Monitoring	Automatisierte Erkennung und qualifizierte Eventverarbeitung
CMDB-Abgleich	Regelmäßiger Abgleich von Asset- und Betriebsdaten
Reporting	Automatisierte Aufbereitung wiederkehrender Servicekennzahlen

Tabelle 9: Automatisierungsfelder

5.4 Zielbild für Segmentierung und Zugriffskontrolle

Die Segmentierung des Netzwerks ist ein wesentliches Sicherheits- und Betriebsprinzip. Der Auftragnehmer muss bestehende Segmentierungsmechanismen betreiben und Weiterentwicklungen so begleiten, dass Betriebsstabilität und Sicherheit gleichermaßen berücksichtigt werden.

Die technische Umsetzung kann je nach Bestand und Zielkomponenten über VLANs, VRFs, ACLs, rollenbasierte Policies, NAC-Attribute oder vergleichbare Mechanismen erfolgen. Entscheidend ist, dass die Zuordnung nachvollziehbar, dokumentiert, getestet und im Störfall analysierbar ist.

Besondere Aufmerksamkeit gilt Medizintechnik, IoT, technischen Anlagen und Sondergeräten. Für diese Geräte sind häufig Ausnahmen, MAB-Verfahren, statische Zuordnungen oder besondere Betriebsabsprachen erforderlich. Solche Ausnahmen müssen kontrolliert und regelmäßig überprüft werden.

5.5 Zielbild für Providerwechselfähigkeit

Der Auftraggeber muss während und nach der Vertragslaufzeit in der Lage sein, den Betrieb zu steuern, zu prüfen und bei Bedarf an einen anderen Betreiber zu übergeben. Providerwechselfähigkeit entsteht nicht am letzten Vertragstag, sondern durch laufende Dokumentations- und Betriebsdisziplin.

Der Auftragnehmer muss deshalb alle wesentlichen Betriebsinformationen in einer Form führen, die für den Auftraggeber nutzbar und exportierbar ist. Hierzu gehören Konfigurationsstände, Assetdaten, Monitoringlogiken, Runbooks, Prozessbeschreibungen, Known Errors und offene Risiken.

6 Technische Leitplanken für Betriebs- und Integrationsfähigkeit

6.1 Zweck der technischen Leitplanken

Dieses Kapitel beschreibt technische Eigenschaften, die aus Sicht des Managed Service für einen sicheren und effizienten Betrieb relevant sind. Es ersetzt keine Hardwarebeschaffung und begründet keine Lieferpflicht des Auftragnehmers.

Die Leitplanken dienen dazu, die Betriebsfähigkeit neuer oder bereitgestellter Komponenten zu bewerten, Integrationsrisiken frühzeitig zu erkennen und spätere Diskussionen über Mindestvoraussetzungen für die Übernahme in den Managed Service zu vermeiden.

6.2 Allgemeine Anforderungen an zu betreibende Komponenten

Anforderung	Bedeutung für den Betrieb
Zentrale Verwaltbarkeit	Komponenten müssen über ein geeignetes Managementverfahren administrierbar sein.
Sichere Administration	Administrative Zugriffe müssen rollenbasiert, personalisiert und protokollierbar sein.
Monitoringfähigkeit	Komponenten müssen mindestens Basisdaten zu Verfügbarkeit, Zustand und Fehlern liefern können.
Konfigurationssicherung	Konfigurationsstände müssen gesichert und wiederhergestellt werden können.
Lifecycle-Transparenz	Supportstatus, Softwarestand und Ersatzoptionen müssen bewertbar sein.
Dokumentierbarkeit	Standort, Rolle, Schnittstellen und Abhängigkeiten müssen in CMDB und Betriebshandbuch abbildbar sein.
Sicherheitsfunktionen	Sichere Protokolle, Authentifizierung und Integritätsschutz müssen entsprechend Komponentenkritikalität verfügbar sein.

Tabelle 10: Cisco-Kompetenzanforderungen

6.3 Core- und Distributionsebene

Core- und Distributionsebene sind für die Gesamtverfügbarkeit des Netzwerks von besonderer Bedeutung. Komponenten in diesen Ebenen müssen so betrieben werden können, dass Wartung, Fehleranalyse, Redundanzprüfung und Wiederherstellung kontrolliert möglich sind.

Der Auftragnehmer muss bei bereitgestellten Komponenten prüfen, ob deren Leistungsfähigkeit, Redundanz, Routingfunktionen, Monitoringfähigkeit und Sicherheitsfunktionen für die vorgesehene Rolle geeignet sind.

- Unterstützung dynamischer Routingverfahren oder anderer abgestimmter Routingmechanismen.
- Redundante Netzteile und Lüfter, soweit für die Rolle erforderlich.
- Geeignete Uplink-Kapazitäten und Link-Aggregation-Mechanismen.
- Fähigkeit zur logischen Trennung von Netzbereichen, z. B. über VRF oder vergleichbare Mechanismen.
- Unterstützung von Telemetrie, Syslog, SNMPv3 oder vergleichbaren Monitoringverfahren.
- Möglichkeit zur sicheren Konfigurationssicherung und Wiederherstellung.

6.4 Access-Ebene

Die Access-Ebene ist die operative Schnittstelle zu Endgeräten. Sie muss im Managed Service besonders gut dokumentiert und standardisiert sein, da Änderungen an Access-Ports unmittelbare Auswirkungen auf Anwender, Medizintechnik und technische Systeme haben können.

Bei neuen oder beigestellten Access-Komponenten ist zu prüfen, ob sie die benötigten Portprofile, PoE-Leistungstufen, Authentifizierungsverfahren, Monitoringdaten und Uplinkkapazitäten bereitstellen können.

- PoE-/PoE+/-/PoE++-Fähigkeit entsprechend Endgeräte- und WLAN-Bedarf.
- 802.1X- und MAC-basierte Authentifizierung für Endgerätezugriff.
- Fallback-Regeln für nicht authentifizierungsfähige oder klinisch sensible Geräte.

- Portprofile für Standardarbeitsplätze, Telefone, Access Points, Medizintechnik, Drucker und Sondergeräte.
- Monitoring von Linkstatus, Fehlerzählern, PoE-Last, MAC-Adressen und Portauslastung.
- Dokumentationsfähigkeit bis auf Port- und Standortebene.

6.5 WLAN-Komponenten

WLAN-Komponenten müssen so integrierbar sein, dass der Auftragnehmer Verfügbarkeit, Performance, Clientverhalten, Funkqualität und Controllerzustände überwachen und auswerten kann. Für den Klinikbetrieb ist WLAN nicht nur Komfortdienst, sondern in vielen Bereichen Teil der operativen Arbeitsfähigkeit.

Bei WLAN-Modernisierungen sind insbesondere SSID-Strukturen, Authentifizierung, Roaming, Kanalplanung, PoE-Versorgung, kritische Bereiche und Dokumentation zu berücksichtigen.

Bei neu installierten oder wesentlich veränderten WLAN-Access-Points ist eine Nachausleuchtung bzw. technische Überprüfung der Funkversorgung durchzuführen, soweit dies für die Abnahme oder den stabilen Betrieb erforderlich ist. Die Ergebnisse sind zu dokumentieren.

Thema	Mindestbetrachtung
SSID-Struktur	Klinik, Verwaltung, Gäste, IoT/Medizintechnik und Sondernetze sind nachvollziehbar zu trennen.
Authentifizierung	802.1X, sichere PSK-Verfahren oder definierte Sonderverfahren müssen dokumentiert sein.
Roaming	Kritische Anwendungen erfordern Betrachtung von Roamingverhalten und Unterbrechungszeiten.
RF-Management	Kanalplanung, Sendeleistung und Interferenzen sind zu überwachen und zu optimieren.
Monitoring	AP-Status, Clientstatus, Signalqualität, Fehlerraten und Controllerzustände sind auszuwerten.

Tabelle 11: SOT-Arbeitspakete

7 Service Ownership Transfer und Due Diligence

7.1 Zielsetzung der SOT-Phase

Die SOT-Phase ist der kontrollierte Übergang vom bisherigen Betrieb in den Managed Service des Auftragnehmers. Sie ist so zu planen, dass der Klinikbetrieb nicht gefährdet wird und der Auftragnehmer am Ende der Phase tatsächlich in der Lage ist, den Betrieb im vereinbarten Umfang zu übernehmen.

Der Auftragnehmer muss die SOT-Phase als eigenes Projekt mit Projektleitung, Meilensteinen, Risiken, Abhängigkeiten und Abnahmekriterien führen. Ein rein informelles Einarbeiten genügt nicht.

7.2 Informationsübernahme

Der Auftraggeber stellt dem Auftragnehmer die verfügbaren Informationen zum Bestand bereit. Der Auftragnehmer darf jedoch nicht davon ausgehen, dass alle Informationen vollständig, aktuell oder widerspruchsfrei sind. Genau aus diesem Grund ist eine strukturierte Due Diligence erforderlich.

Fehlende Informationen sind zu benennen. Der Auftragnehmer muss jeweils beschreiben, ob die fehlende Information betriebsverhindernd, risikorelevant oder lediglich dokumentationsrelevant ist.

Informationsart	Prüfung durch Auftragnehmer
Assetlisten	Vollständigkeit, Dubletten, Standortzuordnung, Seriennummern, Supportstatus
Netzpläne	Plausibilität gegenüber Routing, Uplinks, Standort- und Verteilerstruktur
Konfigurationen	Sicherung, Version, Abweichungen, kritische Sonderkonfigurationen
Monitoring	Abdeckung, Alarmqualität, Schwellenwerte, Eskalationslogik
Tickets	Wiederkehrende Störungen, Top-Ursachen, Eskalationsmuster
Betriebshandbücher	Aktualität, Vollständigkeit, Eignung für Betriebsübernahme

Tabelle 12: SOT-Informationsarten

7.3 SOT-Arbeitspakete

- Projektstart und Kick-off mit Festlegung von Rollen, Kommunikationswegen und Meilensteinen.
- Übernahme und Prüfung der Bestandsdokumentation. Der konkrete Termin wird nach Zuschlag im Rahmen des SOT-Kick-offs zwischen Auftraggeber und Auftragnehmer festgelegt; für die Sichtung ist ein angemessenes Zeitfenster von mindestens einem Arbeitstag vorzusehen.
- Einrichtung sicherer administrativer Zugänge.
- Anbindung an ServiceNow und Festlegung des Ticketflusses.
- Einrichtung bzw. Übernahme der Monitoring- und Alarmierungsinformationen.
- Definition von Incident-, Problem-, Change- und Release-Prozessen.
- Erstellung des initialen Betriebshandbuchs.
- Erstellung der Eskalations- und Kontaktmatrix.
- Risikoregister mit EoL-/EoS-, Dokumentations- und Betriebsrisiken.
- Test der Betriebsprozesse und formale Abnahme der Betriebsübernahme.
- Prüfung der herstellerseitigen Software-Supportfähigkeit der im Scope befindlichen Bestandskomponenten auf Basis der bereitgestellten Asset- und Seriennummerninformationen

7.4 SOT-Ergebnisdokumente

Dokument	Inhalt	Abnahmebezug
SOT-Plan	Zeitplan, Rollen, Arbeitspakete, Abhängigkeiten	Freigabe zu Beginn der SOT
Due-Diligence-Bericht	Bestandsprüfung, Lücken, Risiken, Sofortmaßnahmen	Voraussetzung für Betriebsübernahme
Initiales Betriebshandbuch	Prozesse, Zugriffe, Eskalation, Monitoring, SOPs	Pflichtdokument vor SLA-Start
Risikoregister	Bewertete Risiken inkl. Owner und Maßnahme	Regelmäßiges Review

Dokument	Inhalt	Abnahmebezug
Eskalationsmatrix	Kontakte, Rollen, Zeiten, Managementeskalation	Verbindlich vor Betriebsstart
CMDB-Abgleichplan	Vorgehen zum Datenabgleich	Grundlage für Betriebs- und Abrechnungsdaten

Tabelle 13: SOT-Ergebnisdokumente

7.5 Abnahme der Betriebsübernahme

Die Betriebsübernahme darf nicht stillschweigend angenommen werden. Sie ist formal abzunehmen. Der Auftragnehmer muss nachweisen, dass die technischen und organisatorischen Mindestvoraussetzungen erfüllt sind.

1. Alle im Scope befindlichen Komponenten sind identifiziert oder offene Abweichungen sind dokumentiert.
2. Administrative Zugriffe sind eingerichtet, getestet und protokolliert.
3. Ticketschnittstelle und Meldewege sind funktionsfähig.
4. Monitoring und Alarmierung sind für die vereinbarten Komponenten aktiv.
5. Eskalationsmatrix und Kommunikationswege sind freigegeben.
6. Initiales Betriebshandbuch liegt vor.
7. CMDB-Grunddaten sind übernommen oder Abweichungen sind dokumentiert.
8. Konfigurationssicherung ist eingerichtet oder als Risikopunkt mit Maßnahme dokumentiert.
9. Incident- und Change-Prozess wurden in einem Testfall nachgewiesen.
10. Der Auftraggeber bestätigt den Übergang in den SLA-wirksamen Betrieb.

8 Managed-Service-Grundleistungen

8.1 Betriebsverantwortung

Nach Abnahme der Betriebsübernahme trägt der Auftragnehmer die operative Verantwortung für den vereinbarten Netzwerkbetrieb. Er muss Störungen erkennen, bearbeiten, eskalieren und dokumentieren. Er muss Changes kontrolliert durchführen und den Betrieb so organisieren, dass Servicequalität und Sicherheit nachvollziehbar sind.

Die Betriebsverantwortung bezieht sich auf die vereinbarten Komponenten und Prozesse. Sie entbindet den Auftraggeber nicht von erforderlichen Mitwirkungen, insbesondere bei Freigaben, Zutritt, Bereitstellung von Hardware, Vertragsinformationen, Herstellerzugängen oder Entscheidungen über Risiken.

8.2 Service Desk und NOC

Der Auftragnehmer betreibt einen Service Desk bzw. ein Network Operation Center als zentrale Betriebsinstanz für den Netzwerkservice. Diese Einheit muss qualifiziert besetzt sein und die bestehende Cisco-Infrastruktur technisch verstehen.

Der Service Desk des Auftragnehmers darf nicht als allgemeiner Endanwender-Helpdesk verstanden werden. Der Endanwenderkontakt erfolgt grundsätzlich über den Auftraggeber. Der Auftragnehmer arbeitet mit den vorqualifizierten Meldungen, Monitoringevents und definierten Ansprechpartnern des Auftraggebers.

- Annahme und Bearbeitung vorqualifizierter Incidents.
- Überwachung von Monitoringevents und Alarmeingängen.
- Koordination von 2nd- und 3rd-Level-Ressourcen.
- Koordination von Vor-Ort-Einsätzen.
- Eskalation an Hersteller, Lieferanten oder Drittpartner, soweit erforderlich.
- Statusrückmeldung im führenden ITSM-System.
- Pflege von Knowledge- und Known-Error-Informationen.

8.3 Service Request Management

Service Requests sind planbare, wiederkehrende oder gering komplexe Anforderungen des Betriebs. Der Auftragnehmer muss hierfür einen Service-Request-Katalog bereitstellen und pflegen.

Die verbindliche Ausgestaltung des Service-Request-Katalogs erfolgt in der SOT-Phase gemeinsam mit dem Auftraggeber. Jeder Katalogeintrag ist mit Leistungsinhalt, erforderlichen Angaben und Zielbearbeitungszeit zu hinterlegen. Der Katalog ist im Betriebshandbuch verbindlich zu dokumentieren und mindestens jährlich zu überprüfen.

Service Requests und Changes werden als getrennte Ticketarten geführt, schließen sich jedoch nicht aus: Der Service Request ist das Nachfrage- und Auftragsticket, der Change die Autorisierung einer produktiven Konfigurationsänderung. Wiederkehrende Katalogleistungen mit Konfigurationswirkung werden als Standard Change vorab freigegeben und unter dieser Freigabe ausgeführt; das Request-Ticket verweist auf den freigegebenen Change (Kapitel 13).

Request-Klasse	Kriterium	Zielbearbeitung
SR-1	Im Service-Request-Katalog gelistet; ein Configuration Item betroffen; keine Beteiligung Dritter erforderlich	1 Werktag
SR-2	Im Katalog gelistet; 2 bis 10 Configuration Items betroffen oder Terminabstimmung mit einem Fachbereich erforderlich	3 Werktage
SR-3	Im Katalog gelistet; mehr als 10 Configuration Items oder mehrere Gebäude bzw. Standorte betroffen	5 Werktage
Nicht katalogisiert	Nicht im Katalog enthalten oder Abhängigkeit von Dritten, Hardwarebereitstellung oder baulichen Maßnahmen	Kein Zielwert; Terminabstimmung, ggf. Überführung in das Change-Verfahren

Tabelle 14: Service-Request-Klassen

8.4 Vor-Ort-Unterstützung

Der Auftragnehmer muss Vor-Ort-Unterstützung bereitstellen, wenn eine Störung oder Änderung nicht remote lösbar ist oder wenn physische Tätigkeiten erforderlich sind. Vor-Ort-Leistungen sind insbesondere bei Hardwaredefekten, Uplinkstörungen, Port- und Verkabelungsprüfungen, WLAN-Vermessungen, Inbetriebnahmen oder kritischen Changes relevant.

Die Vor-Ort-Tätigkeit ist mit dem Auftraggeber abzustimmen und im Ticket zu dokumentieren. Zutritts-, Sicherheits- und Hygienevorgaben des Auftraggebers sind einzuhalten.

8.5 Kontinuierliche Verbesserung

Der Auftragnehmer muss den Betrieb kontinuierlich verbessern. Verbesserungen sind nicht ausschließlich als technische Innovation zu verstehen, sondern insbesondere als Reduktion von Störungen, bessere Dokumentation, kürzere Entstörungszeiten, geringere Change-Fehlerquote, weniger Sonderkonfigurationen und höhere Transparenz.

Verbesserungsvorschläge sind im monatlichen Service Report auszuweisen und in den Regelmeetings zu bewerten. Kritische Verbesserungsvorschläge, die Risiken reduzieren oder Sicherheitslücken adressieren, sind gesondert zu eskalieren.

9 ITSM, ServiceNow und Prozessintegration

9.1 Führendes Ticketsystem

Führendes Ticketsystem ist ServiceNow des Auftraggebers. Alle für den Auftraggeber relevanten Bearbeitungsschritte, Statusinformationen, Eskalationen, Freigaben und Abschlussinformationen müssen in ServiceNow nachvollziehbar sein.

Der Auftragnehmer kann eigene interne Systeme einsetzen, sofern dadurch keine Informationsverluste, Medienbrüche oder widersprüchlichen Statusinformationen entstehen. Maßgeblich für die Service- und SLA-Bewertung ist der dokumentierte Stand im führenden System des Auftraggebers.

9.2 Ticketfluss

Incidents werden grundsätzlich durch Monitoring, den Service Desk des Auftraggebers oder definierte Betriebsrollen erzeugt und an den Auftragnehmer übergeben. Mit Übergabe und Annahme des Tickets beginnt die jeweils vereinbarte SLA-Zeit, sofern die Betriebsübernahme erfolgt ist und das Ticket die Mindestinformationen enthält.

Der Auftragnehmer muss den Ticketfluss so gestalten, dass keine manuellen Doppelpflegen erforderlich sind. Übergangsweise kann eine E-Mail-basierte Schnittstelle zulässig sein; Zielzustand ist eine strukturierte Schnittstelle mit Statussynchronisation.

Für die Kalkulation und Dimensionierung des laufenden Managed Service gilt ein jährlicher Orientierungswert von ca. 2.600 Tickets. Diese betreffen insbesondere das Patchen von Datenanschlüssen, VLAN-Anpassungen, Störungsanalyse und Fehlerbehebung sowie sonstige betriebliche Maßnahmen an der Netzwerkinfrastruktur. Der Orientierungswert ist weder eine Mindestabnahmemenge noch eine garantierte Höchst- oder Mindestmenge; die tatsächliche Zuordnung zu den jeweiligen Ticketarten erfolgt nach den UKF-Prozessen.

Ticketinformation	Mindestinhalt
Betroffener Service	LAN, WLAN, Standortanbindung, Core, Distribution, Access, NAC-Schnittstelle oder sonstige Zuordnung
Betroffene Komponente	Hostname, Standort, IP-Adresse, Seriennummer oder eindeutige CI-Zuordnung, soweit verfügbar
Fehlerbild	Beschreibung, Startzeit, Auswirkung, betroffene Nutzer oder Bereiche
Priorität	Initiale Bewertung durch Auftraggeber oder definierte Vorqualifizierung
Kontakt	Technischer Ansprechpartner und Rückmeldeweg
Anhänge	Logs, Screenshots, Monitoringdaten oder relevante Auszüge, soweit vorhanden

Tabelle 15: Mindestinhalt Ticketinformation

9.3 Statussynchronisation

Statusänderungen müssen zeitnah an das führende Ticketsystem zurückgemeldet werden. Dazu gehören insbesondere Annahme, Analysebeginn, Rückfrage, Workaround, Eskalation, Wiederherstellung, Abschlussvorschlag und Abschlussdokumentation.

Tickets dürfen nicht ohne nachvollziehbare technische Begründung geschlossen werden. Die finale Schließung erfolgt durch den Auftraggeber oder gemäß abgestimmtem Prozess.

9.4 CMDB-Integration

Die CMDB des Auftraggebers ist die maßgebliche Referenz für Configuration Items. Der Auftragnehmer muss sicherstellen, dass die für den Betrieb erforderlichen CI-Informationen gepflegt oder zur Pflege bereitgestellt werden.

Änderungen an Komponenten, Standorten, Ports, Softwareständen oder Betriebsrollen müssen im Rahmen des Change- oder Configuration-Managements in die CMDB zurückgeführt werden.

9.5 Prozessqualität

Der Auftragnehmer muss die Qualität der ITSM-Integration regelmäßig überprüfen. Hierzu gehören Auswertungen zu nicht synchronisierten Tickets, fehlenden Pflichtfeldern, offenen Rückfragen, Eskalationsverzug, unvollständigen Abschlussinformationen und nicht gepflegten CIs.

Die Ergebnisse sind Bestandteil des Service Reports.

10 Monitoring, Observability und Reporting

10.1 Ziel des Monitorings

Das Monitoring dient der frühzeitigen Erkennung von Störungen, der Messung der Servicequalität, der Unterstützung von Ursachenanalysen und der Steuerung des Betriebs. Der Auftragnehmer muss Monitoringdaten nicht nur sammeln, sondern bewerten, korrelieren und in handlungsfähige Betriebsinformationen überführen.

Das Monitoring muss die bestehende Cisco-Infrastruktur ebenso abdecken wie später integrierte Komponenten. Unterschiedliche technische Monitoringwege sind zulässig, solange der Auftraggeber eine konsolidierte Sicht auf Servicequalität und Risiken erhält.

10.2 Monitoringumfang

- Core- und Backbone-Komponenten inklusive Redundanzzustand und Uplinks.
- Distribution- und Aggregationssysteme inklusive Routing- und Linkzuständen.
- Access-Switches inklusive Portstatus, Fehlerzähler, PoE-Last und Uplinkzustand.
- WLAN-Controller, Access Points, SSIDs, Clientmetriken und Funkqualität.
- Management- und Monitoringplattformen, soweit für den Netzbetrieb relevant.
- NAC- und AAA-Schnittstellen, soweit sie den Netzwerkzugang beeinflussen.
- Kritische Standort- und Gebäudeverbindungen.
- Konfigurationsänderungen und sicherheitsrelevante Systemmeldungen.

10.3 Mindestmetriken

Metrik	Zweck
Verfügbarkeit	Nachweis der Betriebsfähigkeit je Servicebereich
Interfaceauslastung	Erkennung von Kapazitätsengpässen und Fehlverteilungen
Fehlerzähler	Hinweise auf physische oder logische Verbindungsprobleme
CPU/Speicher	Bewertung der Systembelastung
Temperatur/Hardwarestatus	Früherkennung physischer Komponentenausfälle
PoE-Last	Sicherstellung ausreichender Versorgung für APs, Telefone und Endgeräte
WLAN-Clientdaten	Analyse von Roaming, Signalqualität und Clientproblemen
Konfigurationsänderungen	Nachvollziehbarkeit und Security-Monitoring
Softwarestände	Lifecycle-, Release- und Security-Bewertung

Tabelle 16: Monitoring-Metriken

10.4 Eventkorrelation und Ticket-Spam-Vermeidung

Der Auftragnehmer muss verhindern, dass technische Einzelereignisse ungefiltert zu einer großen Anzahl unqualifizierter Tickets führen. Events sind zu korrelieren, zu priorisieren und technisch einzuordnen.

Beispielhaft darf ein Uplinkausfall nicht gleichzeitig unkoordiniert dutzende Folgealarme für nachgelagerte Geräte als eigenständige Incidents erzeugen, ohne die Abhängigkeitsstruktur zu berücksichtigen. Die Topologie- und Abhängigkeitsinformationen sind daher für das Monitoring relevant.

10.5 Reporting

Der Auftragnehmer erstellt monatliche Service Reports. Die Reports müssen entscheidungsfähig sein und dürfen nicht lediglich Rohdaten aus Monitoring- oder Ticketsystemen enthalten. Der Auftragnehmer muss die Kennzahlen bewerten und Handlungsempfehlungen ableiten.

- SLA-Erfüllung und Abweichungen.
- Verfügbarkeit je Servicebereich und kritischem Netzsegment.
- Ticketvolumen nach Priorität, Kategorie, Standort und Ursache.
- Major Incidents und Root-Cause-Analysen.
- Top-10-Störungsursachen und Wiederholungsfehler.
- Problem-Management-Status.
- Change-Volumen, Change-Erfolg und Change-Folgefehler.
- Firmware-, Software- und Lifecycle-Status.
- EoL-/EoS-Risiken und empfohlene Maßnahmen.
- Kapazitäts- und Performanceentwicklungen.
- Verbesserungsmaßnahmen und offene Mitwirkungspunkte.

10.6 Dashboards und Transparenz

Der Auftraggeber muss Zugriff auf geeignete Dashboards oder Reports erhalten, um den Zustand des Netzwerkservices nachvollziehen zu können. Der Zugriff kann lesend erfolgen und muss so ausgestaltet sein, dass keine unkontrollierten Änderungen durch Dashboardnutzer möglich sind.

Für kritische Bereiche sind nach Möglichkeit gesonderte Sichtweisen bereitzustellen, beispielsweise Core/Backbone, WLAN-KRITIS-Bereiche, Standortanbindungen, PoE-Auslastung und Major-Incident-Lage.

11 Incident Management

11.1 Ziel

Ziel des Incident Managements ist die schnellstmögliche Wiederherstellung der vereinbarten Servicequalität. Dabei ist der klinische Betrieb besonders zu berücksichtigen. Der Auftragnehmer muss zwischen technischer Störung, betrieblicher Auswirkung und klinischer Kritikalität unterscheiden können.

Incidents sind vollständig zu erfassen, zu priorisieren, zu bearbeiten, zu eskalieren und abzuschließen. Die Bearbeitung muss im führenden ITSM-System nachvollziehbar sein.

11.2 Incidentannahme

Incidents können durch Monitoring, durch den Service Desk des Auftraggebers oder durch definierte technische Ansprechpartner entstehen. Der Auftraggeber nimmt eine Vorqualifizierung vor, soweit dies möglich ist. Der Auftragnehmer unterstützt die Vorqualifizierung, wenn eine eindeutige Zuordnung ohne seine Mitwirkung nicht möglich ist.

Der Auftragnehmer muss Incidents nach Eingang unverzüglich prüfen, annehmen und entsprechend der Priorität bearbeiten. Rückfragen dürfen nicht zur Verzögerung der Bearbeitung führen, wenn bereits ausreichende Informationen für erste Maßnahmen vorliegen.

11.3 Priorisierung

Priorität	Beschreibung	Reaktionszeit	Wiederherstellungsziel
P1 Kritisch	Gesamtausfall, Ausfall kritischer Netzwerkbereiche (Switch, Router, etc), erhebliche Wirkung auf Klinikbetrieb oder KRITIS-relevante Prozesse	15 Minuten 24/7	4 Stunden 24/7
P2 Hoch	Ausfall wesentlicher Gebäude-, Service- oder Redundanzfunktionen mit erheblicher Einschränkung	4 Stunden, bei kritischer Wirkung nach Eskalation 24/7	Ende des Werktags bzw. abgestimmt nach Impact
P3 Mittel	Einschränkung einzelner Funktionen oder Komponenten, Workaround möglich	1 Werktag	3 Werktage
P4 Gering	Geringe Beeinträchtigung, kosmetische Fehler oder Dokumentationsabweichung	3 Werktage	Nach Vereinbarung

Tabelle 17: Incident-Prioritäten und SLA

11.4 Major Incident

Ein Major Incident ist ein Vorfall mit erheblicher Auswirkung auf den Klinikbetrieb, zentrale Netzfunktionen oder kritische Versorgungsprozesse. Der Auftragnehmer muss Major Incidents sofort eskalieren und mit priorisierten Ressourcen bearbeiten.

Während eines Major Incidents sind regelmäßige Statusmeldungen erforderlich. Die Frequenz wird im Betriebshandbuch festgelegt und kann durch den Auftraggeber situationsabhängig erhöht werden.

- Sofortige technische Ersteinschätzung.
- Aktivierung der Eskalationskette.
- Bereitstellung qualifizierter 2nd-/3rd-Level-Ressourcen.
- Prüfung und Umsetzung von Workarounds.
- Regelmäßige Lageupdates.
- Dokumentation der Zeitlinie.
- Root-Cause-Analyse nach Wiederherstellung.

11.5 Abschluss und Dokumentation

Ein Incident darf erst abgeschlossen werden, wenn die technische Wiederherstellung dokumentiert und vom Auftraggeber bestätigt oder nach abgestimmtem Prozess akzeptiert wurde. Bei kritischen Incidents ist zusätzlich ein Kurzbericht oder eine RCA erforderlich.

Der Abschluss muss mindestens Ursache, Maßnahme, betroffene Komponenten, Wiederherstellungszeit, verbleibende Risiken und ggf. Folgechanges enthalten.

12 Problem Management

12.1 Ziel

Problem Management dient der nachhaltigen Beseitigung von Ursachen wiederkehrender oder schwerwiegender Störungen. Der Auftragnehmer darf sich nicht darauf beschränken, gleiche Incidents wiederholt einzeln zu beheben.

Wiederkehrende Störungen, auffällige Komponenten, instabile Softwarestände, Change-Folgefehler und strukturelle Dokumentationsmängel sind als Problem zu erfassen und zu bearbeiten.

12.2 Problemklassifikation

Kategorie	Beschreibung	Beispiel
Wiederkehrender Incident	Gleichartige Störungen treten mehrfach auf	Wiederholte WLAN-Abbrüche in einem Gebäudebereich
Strukturelles Risiko	Fehlerursache liegt in Design, Topologie oder Prozess	Kaskadierte Access-Struktur mit hoher Ausfallwirkung
Lifecycle-Problem	Komponente oder Softwarestand verursacht erhöhtes Risiko	EoS-Switch ohne Ersatzteilkonzept
Change-Folgeproblem	Störung entsteht nach Änderung	Fehlerhafte VLAN-Zuordnung nach Change
Dokumentationsproblem	Fehlende oder falsche Information verursacht Betriebsrisiko	Portliste stimmt nicht mit Produktivzustand überein

Tabelle 18: Problem-Kategorien

12.3 Root-Cause-Analyse

Für P1-Incidents ist eine Root-Cause-Analyse verpflichtend. Für P2-Incidents kann der Auftraggeber eine RCA verlangen. Die RCA muss fachlich belastbar sein und darf sich nicht auf allgemeine Aussagen beschränken.

Eine RCA muss die technische Ursache, begünstigende Faktoren, zeitliche Abfolge, betroffene Komponenten, getroffene Maßnahmen, offene Risiken und dauerhafte Präventionsmaßnahmen darstellen.

12.4 Known-Error-Database

Der Auftragnehmer muss eine Known-Error-Database führen. Die KEDB dient dazu, bekannte Fehlerbilder, Workarounds und dauerhafte Maßnahmen nachvollziehbar zu dokumentieren.

Der Auftraggeber erhält Zugriff auf die für den eigenen Betrieb relevanten Inhalte. Ziel ist der Aufbau einer gemeinsamen Wissensbasis, die Vorqualifizierung, Entstörung und Providerwechselfähigkeit verbessert.

12.5 Trendanalyse

Der Auftragnehmer muss monatlich Trends aus Incidents, Problems und Changes ableiten. Die Auswertung muss technische und organisatorische Ursachen berücksichtigen. Reine Ticketstatistik ohne Bewertung genügt nicht.

- Top-10-Störungsursachen je Monat.
- Wiederkehrende Störungen je Standort oder Komponente.
- Change-Folgefehler.
- Instabile Software- oder Firmwarestände.
- Auffällige EoL-/EoS-Komponenten.
- Dokumentations- oder CMDB-Abweichungen mit Betriebswirkung.

13 Change- und Release-Management

13.1 Change Management - Ziel

Das Change Management stellt sicher, dass Änderungen an der Netzwerkumgebung geplant, risikobewertet, freigegeben, durchgeführt, getestet und dokumentiert werden. Änderungen dürfen die Verfügbarkeit und Sicherheit des Klinikbetriebs nicht vermeidbar gefährden.

Jede produktive Änderung an Konfigurationen, Segmenten, Routing, WLAN, Policies, Firmware, Managementsystemen oder Monitoringlogiken ist als Change zu behandeln, sofern sie nicht ausdrücklich als betriebliche Standardhandlung ohne Konfigurationswirkung definiert wurde.

13.2 Verfahrensarten und Change-Typen

Prozessmerkmal	Verbindliches UKF-Wording	Umsetzung
Verfahrensarten	regulärer Change; Emergency Change; Standard Change; Security Change; Info-Change	gemäß Prozessbeschreibung DICT-ChangeManagement
Change-Typen	Minor; Significant; Major	Bewertung nach Kritikalität, Auswirkungen und Risiko gemäß DICT-Prozess
Ausführung durch externen Dienstleister	zusätzliches Request-Ticket als Auftrag	Das Request-Ticket verweist auf den freigegebenen Change und ersetzt weder Change-Antrag noch Freigabe.

Tabelle 19: UKF-Verfahrensarten und Change-Typen

13.3 Mindestinhalt eines Change-Antrags

- Ziel und Anlass des Changes.
- Betroffene Services, Standorte, Komponenten und CIs.
- Technische Umsetzungsschritte.
- Risiko- und Impactbewertung.
- Test- und Validierungsplan.
- Rollback- oder Backout-Plan.
- Kommunikationsplan bei Nutzer- oder Klinikbetriebswirkung.
- Wartungsfenster und Ressourcenplanung.
- Freigaben und beteiligte Rollen.
- Nachweis der erfolgreichen Durchführung.

13.4 CAB und Freigaben

Der Auftragnehmer ist in das Change Advisory Board des Auftraggebers einzubinden. Changes dürfen erst nach Freigabe umgesetzt werden, sofern es sich nicht um einen dokumentierten Emergency Change handelt.

Unvollständige Change-Anträge können durch den Auftraggeber zurückgewiesen werden. Der Auftragnehmer ist verantwortlich für die Qualität der eingereichten Change-Unterlagen.

13.5 Release Management

Der Auftragnehmer muss Hersteller-Releases, Firmwarestände, Security Advisories und Softwareupdates aktiv verfolgen und bewerten. Dabei ist insbesondere zu prüfen, ob ein Release sicherheitsrelevant, stabilitätsrelevant oder funktional erforderlich ist.

Releases dürfen nicht ungeprüft in die produktive Kliniknetzumgebung eingespielt werden. Sie sind zu planen, zu testen, mit Rollback abzusichern und nach Umsetzung zu validieren. Für kritische Security-Fixes ist ein beschleunigtes Verfahren vorzusehen.

13.6 Change-Kennzahlen

Als jährliche Orientierungswerte gelten ca. 4 bis 8 geplante Changes im Zusammenhang mit Firmware- und Softwareupdates der Netzwerkkomponenten, ca. 150 Changes im Zusammenhang mit dem Austausch von Netzwerkkomponenten (insbesondere aufgrund von End-of-Life-/End-of-Support-Ankündigungen der Hersteller) sowie ca. 4 Emergency-Changes pro Jahr. Emergency-Changes sind naturgemäß nicht planbar und können insbesondere aufgrund von Bugfixes, Sicherheitsupdates, Hotfixes oder kritischen Herstellerempfehlungen erforderlich werden; der genannte Wert dient ausschließlich der Orientierung. Die Orientierungswerte sind weder Mindestabnahmemengen noch garantierte Höchst- oder Mindestmengen.

KPI	Bedeutung
Change-Erfolgsquote	Anteil erfolgreich durchgeführter Changes ohne Rollback oder Folgeincident
Change-Folgeincident-Rate	Anteil der Incidents, die nach Changes auftreten
Terminetreue	Durchführung im vereinbarten Wartungsfenster
Rollback-Quote	Häufigkeit erforderlicher Rücknahmen
Unvollständige Change-Anträge	Qualität der Change-Vorbereitung
Emergency-Change-Anteil	Hinweis auf Planungs- oder Stabilitätsprobleme

Tabelle 20: Betriebs-KPIs

14 Configuration Management, CMDB und Dokumentation

14.1 Grundsatz

Ein belastbarer Managed Service ist ohne aktuelle Dokumentation nicht möglich. Der Auftragnehmer muss daher Configuration Management, CMDB-Pflege und Betriebshandbuch als Kernleistung des Managed Service verstehen.

Dokumentation ist nicht nur am Vertragsende relevant. Sie ist Arbeitsgrundlage für Incidentbearbeitung, Changes, Risikoanalysen, Abnahmen, Audits und Providerwechsel.

14.2 CMDB-Pflichtinformationen

Pflichtinformation	Beschreibung
Hostname	Eindeutiger technischer Name der Komponente
Gerätetyp und Rolle	Core, Distribution, Access, WLAN, Controller, Management
Hersteller/Modell	Für Lifecycle, Support und Betrieb relevant
Seriennummer	Für RMA, Wartung und Inventar erforderlich
Standort	Gebäude, Raum, Verteiler, Rack, soweit verfügbar
Managementadresse	IP-Adresse oder Managementpfad
Softwarestand	Firmware/OS-Version und Patchstand
Supportstatus	EoL-/EoS-Datum, Wartungsvertrag, Risiko
Kritikalität	Betriebliche Auswirkung bei Ausfall
Abhängigkeiten	Uplinks, versorgte Bereiche, Services oder redundante Partner

Tabelle 21: CMDB-Pflichtinformationen

14.3 Betriebshandbuch

Der Auftragnehmer muss ein Betriebshandbuch erstellen, pflegen und fortschreiben. Das Betriebshandbuch ist ein verbindliches Betriebsdokument und Bestandteil der laufenden Leistung.

Änderungen am Betrieb, an Rollen, Eskalationen, Schnittstellen, Prozessen oder technischen Standardverfahren sind unverzüglich nachzuziehen. Spätestens fünf Werktage nach Wirksamwerden einer Änderung muss das Betriebshandbuch aktualisiert sein, sofern keine andere Frist vereinbart wird.

- Scope und Komponentenübersicht.
- Rollen und Verantwortlichkeiten.
- Kontakt- und Eskalationsmatrix.
- Incident-, Problem-, Change- und Release-Prozesse.
- Monitoring- und Alarmierungslogik.
- Zugriffs- und Berechtigungskonzept.
- Konfigurationssicherung und Restore-Verfahren.
- SOPs und Runbooks.
- RMA- und Lifecycle-Prozesse.
- Notfall- und Fallbackverfahren.
- Exit-relevante Übergabeinformationen.

14.4 Konfigurationssicherung

Konfigurationsstände produktiver Netzwerkkomponenten sind regelmäßig zu sichern. Die Sicherungen müssen versioniert, nachvollziehbar und im Wiederherstellungsfall verwendbar sein.

Der Auftragnehmer muss regelmäßig prüfen, ob Sicherungen vollständig und wiederherstellbar sind. Für kritische Komponenten sind Restore-Tests oder geeignete Plausibilitätsprüfungen vorzusehen.

14.5 Knowledge Management

Der Auftragnehmer muss eine Knowledge Base pflegen, die wiederkehrende Fehlerbilder, Standardvorgehen, Workarounds, Known Errors und betriebliche Besonderheiten enthält. Die Knowledge Base ist aus Incidents, Problems, Changes und Reviews fortzuschreiben.

Der Auftraggeber erhält Zugriff auf die für seinen Betrieb relevanten Knowledge-Inhalte. Damit soll die eigene Vorqualifizierung verbessert und die Abhängigkeit von Einzelpersonen reduziert werden.

15 Security, Zugriff und Schnittstellen zu Sicherheitsprozessen

15.1 Sicherheitsgrundsatz

Der Netzwerkbetrieb ist Teil der Sicherheitsarchitektur des Auftraggebers. Der Auftragnehmer muss alle Betriebsleistungen so erbringen, dass Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit gewährleistet bleiben.

Der Auftragnehmer muss die Sicherheitsrichtlinien des Auftraggebers einhalten und seine Mitarbeitenden entsprechend verpflichten. Administrative Tätigkeiten sind nachvollziehbar zu dokumentieren.

15.2 Administrative Zugriffe

- Administrative Zugriffe erfolgen ausschließlich über freigegebene Zugangswege.
- Zugänge sind personalisiert und dürfen nicht als gemeinsam genutzte Standardkonten betrieben werden.
- Multi-Faktor-Authentifizierung ist für Remotezugriffe verpflichtend.
- Berechtigungen sind rollenbasiert zu vergeben und regelmäßig zu überprüfen.
- Administrative Aktionen sind zu protokollieren.
- Ausscheidende oder wechselnde Mitarbeitende des Auftragnehmers sind unverzüglich aus den Berechtigungen zu entfernen.

15.3 Zugriff des Auftraggebers

Der Auftraggeber behält für definierte, geschulte Mitarbeitende administrative Zugriffsmöglichkeiten auf Netzwerkkomponenten und Managementsysteme. Dies dient der Notfallfähigkeit, der technischen Steuerung, der Nachvollziehbarkeit und dem Erhalt interner Kernkompetenz.

Diese Zugriffsmöglichkeit begründet keinen Co-Managed-Regelbetrieb. Eingriffe des Auftraggebers in produktive Systeme sind nach den vereinbarten Prozessen zu dokumentieren.

15.4 Security Incidents

Der Auftragnehmer muss sicherheitsrelevante Netzwerkereignisse erkennen, bewerten und an die definierten Sicherheitsrollen des Auftraggebers melden. Dazu gehören insbesondere verdächtige Portaktivitäten, auffällige WLAN-Clients, NAC-Verstöße, unautorisierte Konfigurationsänderungen, ungewöhnliche Trafficmuster und relevante Hersteller-Sicherheitsmeldungen.

Die Zusammenarbeit mit SOC/SIEM, Informationssicherheit und Datenschutz des Auftraggebers ist im Betriebshandbuch zu beschreiben. Der Auftragnehmer muss Maßnahmen zur Eindämmung oder Isolation unterstützen, wenn diese durch den Auftraggeber freigegeben oder im Notfallprozess vorgesehen sind.

15.5 Datenschutz und Vertraulichkeit

Der Auftragnehmer kann im Rahmen des Netzwerkbetriebs Zugriff auf technische Daten, Nutzungsdaten, personenbezogene Informationen oder sicherheitsrelevante Informationen erhalten. Der Umgang mit diesen Daten muss den Datenschutz- und Vertraulichkeitsanforderungen des Auftraggebers entsprechen.

Verarbeitungsorte, Subunternehmer, Zugriffswege, Protokolldaten und Löschverfahren sind auf Anforderung offenzulegen. Daten des Auftraggebers dürfen nicht ohne Freigabe außerhalb der vereinbarten Verarbeitungs- und Supportwege verarbeitet werden.

16 Modernisierungs- und Integrationsleistungen

16.1 Grundsatz

Die Modernisierung der Netzwerkinfrastruktur bleibt fachlich relevant, wird jedoch nicht als Hardwarelieferungsverpflichtung des Auftragnehmers verstanden. Der Auftragnehmer unterstützt den Auftraggeber bei der Planung, Integration und Betriebsübernahme bereitgestellter oder separat beschaffter Komponenten.

Die Integrationsleistung ist Teil des Managed-Service-Kontextes, weil neue Komponenten nur dann ihren Nutzen entfalten, wenn sie sauber in Monitoring, CMDB, Betriebshandbuch, Change-Prozesse und Service Levels übernommen werden.

16.2 Integrationsprozess

Schritt	Inhalt	Ergebnis
1 Vorprüfung	Prüfung der Komponente, Lizenz, Software, Supportstatus und Zielrolle	Übernahmebewertung
2 Planung	Umsetzungsplan, Wartungsfenster, Risiko, Rollback, Kommunikationsbedarf	Freigegebener Integrationsplan
3 Vorbereitung	Konfiguration, Templates, Monitoringvorbereitung, CMDB-Vorbereitung	Bereit zur Inbetriebnahme
4 Umsetzung	Einbau-/Inbetriebnahmeunterstützung, Konfiguration, Tests	Technisch produktiv
5 Abnahme	Funktionstest, Monitoring, Dokumentation, Konfigurationssicherung	Formale Betriebsübernahme
6 Stabilisierung	Nachbeobachtung, Fehlerkorrektur, Lessons Learned	Regelbetrieb

Tabelle 22: Konfigurationssicherung Schritte

16.3 Zielbild- und Umsetzungskonzept

Der Auftragnehmer muss nach der Stabilisierungsphase ein Zielbild- und Umsetzungskonzept erstellen. Dieses Konzept dient als Arbeitsgrundlage für spätere Modernisierungsmaßnahmen und für die Steuerung der Betriebsentwicklung.

Das Konzept muss nicht alle Details einer späteren Hardwarebeschaffung ersetzen. Es muss jedoch so konkret sein, dass Anforderungen an Betrieb, Integration, Monitoring, Standardisierung, Migration und Abnahme ableitbar sind.

Die Zielarchitektur und die daraus abgeleiteten Integrations- und Modernisierungsmaßnahmen müssen so ausgerichtet sein, dass ein künftig stärker softwaregestütztes, logisch segmentiertes und zentral steuerbares Campus-Betriebsmodell unterstützt wird. Hierzu gehören insbesondere die Fähigkeit zur logischen Trennung von Netzbereichen, die Integration von NAC- und Rolleninformationen, standardisierte Port- und Betriebsprofile, dynamische oder vergleichbar automatisierbare Routing- und Segmentierungsmechanismen sowie eine zentrale Management-, Monitoring- und Dokumentationsfähigkeit. Eine herstellereigenspezifische Technologie wird nicht vorgegeben; maßgeblich ist die funktionale Eignung für eine schrittweise Weiterentwicklung des Bestandsnetzes in Richtung eines automatisierbaren, segmentierungsfähigen und zentral steuerbaren Zielbetriebes.

- Bewertung des bestehenden Netzwerkdesigns.
- Vorschlag zur Reduktion betrieblicher Komplexität.
- Standardisierungs- und Automatisierungsfahrplan.
- Segmentierungs- und NAC-Weiterentwicklung.
- Empfehlung zur Reihenfolge von Modernisierungswellen.
- Abhängigkeiten von passiver Infrastruktur und Drittleistungen.
- Abnahmekriterien je Netzbereich.
- Risiko- und Rollbackbetrachtung.

16.4 Parallelbetrieb CMO/FMO

Während der Vertragslaufzeit können CMO- und FMO-Bereiche parallel bestehen. Der Auftragnehmer muss beide Betriebszustände beherrschen und sauber voneinander abgrenzen.

Für jeden Netzbereich ist nachvollziehbar zu dokumentieren, welchem Betriebsmodus er zugeordnet ist, welche Servicequalität gilt, welche Komponenten enthalten sind und welche offenen Risiken bestehen.

16.5 Abhängigkeiten und Mitwirkungen

Modernisierungs- und Integrationsleistungen können von Faktoren abhängen, die außerhalb des Einflussbereichs des Auftragnehmers liegen. Hierzu gehören insbesondere Lieferzeiten, passive Verkabelung, bauliche Maßnahmen, Zugang zu Verteilerräumen, Freigaben, Drittprovider und klinische Sperrzeiten.

Der Auftragnehmer muss solche Abhängigkeiten frühzeitig melden und im Meilensteinplan berücksichtigen. Verzögerungen dürfen nicht erst nach Ablauf von Fristen angezeigt werden.

16.6 TMO – Übeführung vom Legacy-LAN in das Zielbetriebsmodell

Die nachfolgenden TMO-Phasen konkretisieren ausschließlich die gesondert in der Preismatrix ausgewiesenen einmaligen Überführungsleistungen in das Zielbetriebsmodell. Sie ersetzen nicht die Regelungen zu SOT, laufendem Managed Service, Change Management, Monitoring, Configuration Management, Dokumentation, Abnahme oder Abrechnung, sondern wenden diese Regelungen auf die jeweilige Übeführung eines Netzbereichs an.

Leistungen, die gemäß Kapitel 20.5 und 20.6 Bestandteil der laufenden CMO-/FMO-Portpauschalen sind, werden durch Kapitel 16.6 nicht erneut gesondert vergütet. Kapitel 16.6 beschreibt ausschließlich die strukturierte Übeführung eines Netzbereichs, einer Komponentengruppe oder größerer Portmengen in ein freigegebenes Ziel- und Betriebsdesign.

Das Zielbetriebsmodell orientiert sich funktional an einem modernen, softwaredefinierten Campus-/Fabric-Betriebsmodell. Hierzu gehören insbesondere zentrale Design- und Provisionierungslogiken, standardisierte Port- und Betriebsprofile, virtuelle bzw. logisch getrennte Netzbereiche, rollen- und policybasierte Zugriffskontrolle, Integration von NAC-/AAA-Informationen sowie ein durchgängiges Management-, Monitoring- und Dokumentationsmodell. Eine herstellereigenspezifische Technologie wird damit nicht vorgegeben; maßgeblich ist die funktionale Eignung für einen schrittweise modernisierbaren, segmentierungsfähigen und zentral steuerbaren Campusbetrieb.

Der grundsätzliche Migrationspfad lautet: Legacy-LAN / CMO → High-Level-Design Zielbetrieb → Low-Level-Design → Pilot / technische Validierung → Rollout-Planung → paralleler Pilotbetrieb → stufenweise Migration → formale Übernahme in den FMO.

Der CMO-Betrieb bleibt während der Übeführung aufrechterhalten, bis der jeweilige Netzbereich erfolgreich getestet, dokumentiert, in die Betriebsprozesse übernommen und durch den Auftraggeber abgenommen wurde. Eine automatische Zuordnung zum FMO allein durch Hardwaretausch oder technische Inbetriebnahme findet nicht statt.

Eine nicht erfolgreiche oder unvollständige TMO-Umsetzung verhindert die Abnahme des jeweiligen Übeführungsabschnitts und dessen Zuordnung zum FMO. Der betreffende Netzbereich verbleibt bis zur erfolgreichen Nachbesserung und Abnahme im CMO bzw. in dem zuletzt freigegebenen Betriebszustand.

Die TMO-Leistungen werden in der Preismatrix, Tabellenblatt „TMO“, als gesonderte Leistungspositionen ausgewiesen und nach Personentagen kalkuliert. Reisezeiten, An- und Abfahrtskosten sowie Übernachtungskosten sind in den angebotenen Tagessätzen enthalten und werden nicht gesondert vergütet. Ein Abruf erfolgt nur für durch den Auftraggeber freigegebene Übeführungspakete.

Nicht Bestandteil der TMO-Leistungen sind Hardwarelieferungen, passive Infrastrukturmaßnahmen, bauliche Leistungen, Lizenz- oder Subscription-Kosten, Herstellerwartungskosten sowie Leistungen, die bereits ausdrücklich über die laufenden CMO-/FMO-Portpauschalen abgegolten sind, sofern sie nicht in der Preismatrix gesondert ausgewiesen oder durch den Auftraggeber ausdrücklich beauftragt werden.

16.6.1 Grobplanung und High-Level-Design

Der Auftragnehmer erstellt für die Übeführung in das Zielbetriebsmodell eine Grobplanung und ein High-Level-Design. Grundlage hierfür sind das Zielbild- und Umsetzungskonzept gemäß Kapitel 16.3, die Ergebnisse der SOT- und Stabilisierungsphase sowie die durch den Auftraggeber freigegebenen Rahmenbedingungen.

Im Rahmen der Grobplanung erfasst der Auftragnehmer die relevanten Netzwerk-Use-Cases, Betriebsanforderungen, Segmentierungsanforderungen, Abhängigkeiten, Standort- und Gebäudestrukturen sowie Anforderungen an Management, Monitoring, NAC-/AAA-Integration, Dokumentation und Abnahme.

Das High-Level-Design beschreibt die Zielstruktur auf einer fachlich und technisch nachvollziehbaren Ebene. Es muss insbesondere aufzeigen, wie der bisherige Legacy-LAN-Betrieb schrittweise in ein softwaregestütztes, logisch segmentiertes und zentral steuerbares Campus-Betriebsmodell übeführt werden kann.

Das High-Level-Design enthält mindestens die Abgrenzung des Übeführungspakets, die betroffenen Standorte, Gebäude, Verteilbereiche, Komponenten und Portgruppen, die vorgesehenen Betriebs-, Port- und Rollenprofile, die Grundsätze der logischen Netztrennung und Zugriffskontrolle, die Schnittstellen zu NAC, AAA, Monitoring, ITSM und CMDB sowie einen Grobterminplan mit Migrationswellen, Abhängigkeiten und Entscheidungspunkten.

Ergebnis dieser Phase sind ein abgestimmtes High-Level-Design, ein Grobterminplan, eine Abhängigkeitsübersicht sowie die Festlegung der Entscheidungs- und Freigabeverantwortlichen für die nachfolgenden Phasen.

16.6.2 System Design / Low-Level-Design

Vor Beginn der produktiven Übeführung ist ein Low-Level-Design zu erstellen. Ziel ist es, die technische Umsetzung so weit zu konkretisieren, dass die Migration kontrolliert, reproduzierbar, testbar und rückrollbar durchgeführt werden kann.

Das Low-Level-Design konkretisiert das High-Level-Design für den jeweiligen Übeführungsbereich. Es berücksichtigt insbesondere die bestehenden Konfigurationen, VLAN-/VRF- bzw. Segmentierungslogik, Portbelegungen, Uplink- und Redundanzstrukturen, Routingbeziehungen, WLAN-Abhängigkeiten, NAC-/AAA-Anbindungen, Monitoringpunkte sowie bestehende Sonderkonfigurationen.

Das Low-Level-Design umfasst mindestens die technischen Zielkonfigurationen für die betroffenen Komponenten und Portgruppen, IP-, VLAN-, VRF-, Routing- und Segmentierungsinformationen, virtuelle bzw. logisch getrennte Netzbereiche, Port-, Betriebs- und Rollenprofile, NAC-/AAA- und Authentifizierungslogik, Monitoring-, Logging- und Telemetrieanforderungen, Testfälle sowie Cutover- und Rollback-Vorgaben.

Die schriftliche Freigabe des Low-Level-Designs durch den Auftraggeber ist Voraussetzung für den Beginn der produktiven Umsetzung des jeweiligen Übeführungspakets.

16.6.3 Vorbereitung Pilot / technische Validierung

Vor einer produktiven Migration bereitet der Auftragnehmer einen Pilot- bzw. Validierungsbereich vor. Dieser dient dazu, das Zielbetriebsmodell technisch und betrieblich in einem abgegrenzten Umfang zu prüfen, bevor eine breitere Übeführung erfolgt.

Die Vorbereitung umfasst insbesondere die Festlegung des Pilotumfangs und der Abgrenzung zum Produktivbetrieb, die Vorbereitung der erforderlichen Netzwerk-, Management- und Betriebsfunktionen, die Definition der benötigten Fabric-/Overlay-, Segmentierungs- oder vergleichbaren Zielbetriebsfunktionen sowie die Vorbereitung der Schnittstellen zu Core-/Routing, NAC/AAA, Monitoring, ITSM und CMDB.

Der Pilotbereich ist so zu wählen, dass die wesentlichen Funktionen des Zielbetriebs nachvollziehbar geprüft werden können, ohne den Klinikbetrieb vermeidbar zu gefährden.

16.6.4 PoC / technische Validierung

Der Auftragnehmer führt für den definierten Pilot- bzw. Validierungsbereich einen Proof of Concept oder eine vergleichbare technische Validierung durch. Ziel ist es, kritische Funktionen, Schnittstellen und Betriebsabläufe vor produktiver Umsetzung zu prüfen.

Zu prüfen sind insbesondere Erreichbarkeit und Routingverhalten, logische Netztrennung und Segmentierung, rollen- und policybasierte Zugriffskontrolle, NAC-/AAA-Integration, Management-, Monitoring- und Loggingintegration, Verhalten bei Ausfall- und Redundanzszenarien, Rollback-Fähigkeit, Auswirkungen auf bestehende CMO-Bereiche sowie Betriebsfähigkeit im Zusammenspiel mit ServiceNow, CMDB und Betriebshandbuch.

Die Ergebnisse sind zu dokumentieren. Festgestellte Abweichungen sind zu bewerten und in das Low-Level-Design sowie in den Migrationsplan einzuarbeiten. Die erfolgreiche technische Validierung ist Voraussetzung für die produktive Migration, sofern der Auftraggeber diese für das jeweilige Übeführungspaket verlangt.

16.6.5 Migration Plan / Rollout-Planung und Runbook

Nach Abschluss des Low-Level-Designs und der technischen Validierung erstellt der Auftragnehmer die Rollout-Planung für die produktive Übeführung.

Die Rollout-Planung beschreibt die konkrete Reihenfolge, in der die betroffenen Netzbereiche, Verteilbereiche, Komponentengruppen oder Portmengen in das Zielbetriebsmodell übeführt werden. Die Planung muss so erfolgen, dass Risiken für den Klinikbetrieb minimiert, Abhängigkeiten beherrscht und Rückfallmöglichkeiten erhalten bleiben.

Der Auftragnehmer erstellt hierzu ein Runbook. Dieses enthält mindestens Migrationswellen und Reihenfolge der Übeführung, betroffene Komponenten, Ports, Standorte und Betriebsbereiche, technische Umsetzungsschritte, Verantwortlichkeiten und Mitwirkungen, Wartungsfenster und Sperrzeiten, Kommunikations- und Eskalationswege, Test- und Abnahmeschritte je Migrationswelle, Rollback-Kriterien, Dokumentations- und CMDB-Aktualisierung sowie Übergabekriterien in den FMO-Betrieb.

Das Runbook ist vor Beginn der Migration mit dem Auftraggeber abzustimmen und freizugeben.

16.6.6 Paralleler Pilotbetrieb

Vor einer breiteren Umsetzung ist ein repräsentativer Pilotbetrieb durchzuführen, sofern dies aufgrund von Umfang, Risiko oder Komplexität der Übeführung erforderlich ist. Der Pilotbetrieb dient als Referenz für weitere Übeführungswellen.

Im parallelen Pilotbetrieb werden CMO- und Zielbetriebsmodell kontrolliert nebeneinander betrieben. Ziel ist es, die Zielarchitektur unter realitätsnahen Bedingungen zu prüfen und gleichzeitig Rückfallmöglichkeiten in den bisherigen Betriebszustand aufrechtzuerhalten.

Im Pilotbetrieb sind mindestens Erreichbarkeit und Performance, Segmentierung und Zugriffskontrolle, Authentifizierung über NAC/AAA, Monitoring, Logging und Alarmierung, Ticket- und Eskalationswege, Konfigurationssicherung, Betriebsdokumentation, CMDB-Aktualität sowie Rollback- und Fallbackfähigkeit zu prüfen.

Der Pilotbetrieb ist für einen mit dem Auftraggeber abgestimmten Zeitraum zu beobachten. Auffälligkeiten sind zu dokumentieren, zu bewerten und vor Beginn weiterer Migrationswellen zu beheben oder als freigegebenes Restrisiko zu kennzeichnen.

Erkenntnisse aus dem Pilotbetrieb sind in Rollout-Planung, Runbooks, Betriebshandbuch, Testpläne und Dokumentation zu übernehmen.

16.6.7 Rollout und Migration in den Zielbetrieb

Nach erfolgreicher Pilotierung erfolgt der stufenweise Rollout des Zielbetriebsmodells. Die Migration erfolgt in abgegrenzten Teilbereichen, z. B. je Gebäude, Verteilbereich, Komponentengruppe oder Portgruppe.

Die Migration umfasst insbesondere die Vorbereitung der Zielkonfigurationen, die Abstimmung und Freigabe der Wartungsfenster, die technische Umsetzung, die Migration bestehender Konfigurationen in das

freigegebene Zielmodell, die Anpassung von Port-, Betriebs-, Segmentierungs- und Monitoringprofilen, die Herstellung der Management-, Monitoring-, CMDB- und ITSM-Integration sowie die Durchführung definierter Funktions- und Erreichbarkeitstests.

Während der Migration stellt der Auftragnehmer den geordneten Parallelbetrieb zwischen CMO- und FMO-Bereichen sicher. Änderungen sind über das Change Management zu steuern. Kritische Abweichungen, nicht erfolgreiche Tests oder erhöhte Betriebsrisiken sind unverzüglich an den Auftraggeber zu eskalieren.

Ein Netzbereich gilt erst dann als technisch überführt, wenn die definierten Tests erfolgreich durchgeführt, die Dokumentation aktualisiert, die Monitoring- und CMDB-Anbindung hergestellt und die Abnahmevoraussetzungen erfüllt sind.

16.6.8 Workshops und Know-how-Transfer

Der Auftragnehmer führt im Rahmen der TMO-Leistungen projektbegleitende Workshops und Know-how-Transfer für die benannten Mitarbeitenden des Auftraggebers durch.

Ziel ist es, den Auftraggeber in die Lage zu versetzen, das Zielbetriebsmodell fachlich nachzuvollziehen, Betriebsentscheidungen zu bewerten, Freigaben sachgerecht zu erteilen und im Notfall handlungsfähig zu bleiben.

Die Workshops umfassen mindestens Zielarchitektur und Betriebsmodell, Port-, Betriebs- und Rollenprofile, Segmentierungs- und Zugriffskontrollmodell, NAC-/AAA-Anbindung, Management-, Monitoring- und Loggingprozesse, Change-, Rollback- und Abnahmeverfahren, Troubleshooting-Grundlagen für den Zielbetrieb sowie Dokumentation, CMDB und Betriebshandbuch.

Die Wissensvermittlung erfolgt in deutscher Sprache. Umfang, Format, Teilnehmerkreis und Termine werden mit dem Auftraggeber abgestimmt. Die Durchführung ist zu dokumentieren.

16.6.9 Dokumentation und Betriebsübernahme

Der Auftragnehmer erstellt und übergibt für jedes Übeführungspaket eine vollständige, prüffähige Projekt- und Betriebsdokumentation. Die Dokumentation muss so erstellt werden, dass der übeführte Netzbereich unmittelbar in den FMO-Betrieb übernommen werden kann.

Die Dokumentation umfasst mindestens freigegebenes High-Level-Design, freigegebenes Low-Level-Design, Migrations- und Cutover-Plan, Rollback-Plan, Test- und Abnahmeprotokolle, aktualisierte Netz- und Schnittstellendokumentation, Port-, VLAN-/VRF-, Segmentierungs- und Profilinformatoren, Konfigurationsstände und Sicherungsnachweise, Monitoring- und Alarmierungsinformationen, CMDB-relevante Daten, Betriebs- und Supportzuständigkeiten sowie offene Punkte, Restrisiken und empfohlene Folgemaßnahmen.

Die Dokumentation ist in digitaler, weiterverarbeitbarer Form bereitzustellen. Sie ist spätestens mit Abschluss der jeweiligen Übeführung zu aktualisieren und dem Auftraggeber zur Abnahme vorzulegen.

16.6.10 Projektmanagement der TMO-Leistungen

Der Auftragnehmer benennt dem Auftraggeber vor Beginn der TMO-Leistungen einen verantwortlichen Projektleiter. Der Projektleiter ist zentrale Ansprechperson für Planung, Steuerung, Reporting, Ressourcenkoordination und Eskalation der Übeführungsleistungen.

Zu den Aufgaben des Projektleiters gehören insbesondere Erstellung und Pflege des Projektzeitplans, Koordination der technischen und organisatorischen Ressourcen, Steuerung von Abhängigkeiten, Risiken und offenen Punkten, Vorbereitung und Durchführung von Projekt- und Statusmeetings, Reporting zum Projektfortschritt, Eskalation bei Termin-, Qualitäts-, Ressourcen- oder Betriebsrisiken sowie Koordination von Freigaben, Wartungsfenstern und Abnahmen.

Das Projektmanagement wird in der Preismatrix als eigene TMO-Position ausgewiesen. Die Aufgaben des Projektleiters enden für das jeweilige Übeführungspaket mit der formalen Abnahme und Übergabe in den FMO-Betrieb, soweit keine abweichende Vereinbarung getroffen wird.

16.6.11 Risiko- und Pufferposition

Für unvorhergesehene Aufwände im Rahmen der TMO-Leistungen kann in der Preismatrix eine Risiko- und Pufferposition vorgesehen werden. Diese Position dient ausschließlich der Abdeckung sachlich begründeter Mehraufwände innerhalb freigegebener Überführungspakete.

Ein Abruf der Pufferposition ist nur nach vorheriger schriftlicher Freigabe durch den Auftraggeber zulässig. Der Auftragnehmer hat den Bedarf vor Abruf nachvollziehbar zu begründen und die betroffenen Arbeitspakete, Ursachen, Auswirkungen und erwarteten Zusatzaufwände darzustellen.

Die Pufferposition darf nicht zur Abrechnung von Aufwänden verwendet werden, die bei ordnungsgemäßer Planung, Prüfung und Kalkulation vorhersehbar gewesen wären. Nicht abgerufene Puffertage werden nicht vergütet.

Nicht über die Pufferposition abrechenbar sind Hardwarelieferungen, Lizenz- oder Subscriptionkosten, Herstellerwartung, passive Infrastrukturmaßnahmen, bauliche Leistungen sowie laufende Betriebsleistungen, die bereits über die CMO-/FMO-Portpauschalen abgegolten sind.

17 Lifecycle-, EoL-/EoS- und RMA-Management

17.1 Lifecycle-Management

Der Auftragnehmer muss den technischen Lifecycle der betreuten Netzwerkkomponenten aktiv überwachen. Dies umfasst Supportstatus, EoL-/EoS-Daten, Firmwarestände, Security Advisories, Ersatzteilverfügbarkeit und betriebliche Risiken.

Lifecycle-Management ist eine laufende Pflicht des Managed Service. Es reicht nicht aus, nur bei einem Hardwaredefekt oder Security Incident auf fehlenden Support hinzuweisen.

17.2 EoL-/EoS-Register

Der Auftragnehmer führt ein EoL-/EoS-Register für die betreuten Komponenten. Das Register ist mindestens quartalsweise zu aktualisieren und bei kritischen Herstellerinformationen anlassbezogen fortzuschreiben.

Datenfeld	Beschreibung
Komponente	Hostname, Modell, Seriennummer und Standort
Supportstatus	Aktueller Herstellerstatus und relevantes Datum
Kritikalität	Auswirkung bei Ausfall oder Sicherheitslücke
Risiko	Technisches, betriebliches oder sicherheitsbezogenes Risiko
Empfehlung	Weiterbetrieb, Austausch, Workaround, Monitoringmaßnahme
Owner	Verantwortliche Rolle für Entscheidung oder Maßnahme
Termin	Empfohlener Umsetzungszeitpunkt

Tabelle 23: CMDB-Datenfelder

17.3 RMA-Rolle des Auftragnehmers

Da Hardwarelieferung und Herstellerwartung grundsätzlich nicht Gegenstand dieses Leistungsverzeichnisses sind, ist die RMA-Rolle des Auftragnehmers als Betriebs- und Koordinationsrolle ausgestaltet.

Der Auftragnehmer diagnostiziert Defekte, grenzt betroffene Komponenten ein, empfiehlt Austauschmaßnahmen, koordiniert mit dem Auftraggeber und ggf. mit separaten Hardware- oder Wartungspartnern, unterstützt die Wiederinbetriebnahme und dokumentiert den Vorgang.

Der Auftragnehmer garantiert nicht die Lieferfähigkeit von Ersatzhardware, sofern er diese nicht ausdrücklich als separate Leistung bereitstellen muss. Er muss jedoch frühzeitig auf fehlende Spares, fehlende Wartungsgrundlagen oder kritische Ersatzteilrisiken hinweisen.

17.4 Spares- und Ersatzteilkonzept

Der Auftragnehmer muss dem Auftraggeber auf Basis der Kritikalität der Komponenten Empfehlungen für ein Spares- oder Ersatzteilkonzept geben. Diese Empfehlungen sind insbesondere für Core-, Distribution-, WLAN-Controller-, kritische Access- und KRITIS-relevante Bereiche erforderlich.

Die Entscheidung über Beschaffung und Vorhaltung liegt beim Auftraggeber, soweit keine gesonderte Beauftragung des Auftragnehmers erfolgt.

17.5 Umgang mit nicht supporteten Komponenten

Nicht supportete Komponenten können weiterhin Bestandteil des CMO sein, solange der Auftraggeber sie produktiv betreibt. Der Auftragnehmer muss den Betrieb nach bestem fachlichem Können unterstützen, gleichzeitig aber die Einschränkungen transparent dokumentieren.

Für solche Komponenten können im Einzelfall angepasste Wiederherstellungsannahmen erforderlich werden. Diese müssen ausdrücklich dokumentiert und vom Auftraggeber bestätigt werden. Eine pauschale Entlastung des Auftragnehmers ist nicht zulässig.

Ist ein herstellerbezogener Software-Support für eine Komponente nicht oder nur nach kostenpflichtiger Nachregistrierung, Reinstatement oder Übertragung verfügbar, hat der Auftragnehmer dies unverzüglich anzuzeigen und eine Freigabe des Auftraggebers einzuholen. Zeiträume, in denen ein erforderlicher

Herstellersupport aus Gründen, die der Auftragnehmer nicht zu vertreten hat, trotz rechtzeitiger Anzeige und Freigabeanforderung nicht zur Verfügung steht, gelten als entschuldbare Leistungsminderung nach Kapitel 18.5. Eine darüber hinausgehende pauschale Aussetzung der Service Level erfolgt nicht.

17.6 Herstellerbezogener Software-Support, Bugfixes und Updates

- Für die im Leistungsumfang befindlichen Bestandskomponenten ist ein geeigneter herstellerbezogener Software-Support vorzusehen, soweit dieser für den sicheren und stabilen Betrieb der jeweiligen Komponente erforderlich und herstellerseitig verfügbar ist.
- Der Software-Support umfasst insbesondere den Zugriff auf sicherheits- und stabilitätsrelevante Bugfixes, Patches, Software-/Firmware-Updates, Security Advisories sowie die fachliche Bewertung und kontrollierte Einspielung dieser Updates im Rahmen des Change- und Release-Managements.
- Die Position umfasst keine Lieferung aktiver Hardware und keinen pauschalen herstellerseitigen Ersatzteilservice. Integrations-, Austausch- und Betriebsübernahmeleistungen für durch den Auftraggeber bereitgestellte oder separat beschaffte Hardware bleiben hiervon unberührt und sind gemäß den Regelungen zu Modernisierungs-, Integrations- und Change-Leistungen zu erbringen.
- Der Auftragnehmer hat im Rahmen der Betriebsübernahme zu prüfen, für welche Komponenten ein solcher Software-Support herstellerseitig verfügbar ist. Hierfür stellt der Auftraggeber im weiteren Verfahren bzw. nach Zuschlag die erforderlichen Asset-Informationen, insbesondere Seriennummern, zur Verfügung.
- Für die Kalkulation des herstellerbezogenen Software-Supports hat der Bieter die in Kapitel 4.10 dargestellten Lifecycle-Informationen zugrunde zu legen. Komponenten, deren End-of-Service-Datum zum Zeitpunkt des Leistungsbeginns bereits abgelaufen ist, sind nicht Gegenstand des herstellerbezogenen Software-Supports; für diese Komponenten gelten die Regelungen gemäß Kapitel 17.5. Komponenten, deren End-of-Service-Datum in die Vertragslaufzeit fällt, sind nur bis zum jeweiligen End-of-Service-Datum zu kalkulieren; danach gelten ebenfalls die Regelungen gemäß Kapitel 17.5. Die in der Preismatrix ausgewiesenen Wertungsmengen und Wertungslaufzeiten berücksichtigen diese Differenzierung. Die tatsächliche Abrechnung erfolgt auf Basis der im Rahmen der SOT-Phase verifizierten Asset- und Supportinformationen und nur für Komponenten, für die ein herstellerseitiger Software-Support tatsächlich verfügbar und durch den Auftraggeber freigegeben ist.
- Unterschiedliche Laufzeiten von Software-, Subskriptions- oder Supportansprüchen sind durch den Auftragnehmer im Rahmen der Betriebsübernahme transparent aufzunehmen. Soweit sinnvoll, hat der Auftragnehmer dem Auftraggeber Vorschläge zur Harmonisierung von Lizenz- und Supportlaufzeiten, insbesondere durch Co-Terminierung oder gleichwertige herstellerübliche Verfahren, vorzulegen. Kostenpflichtige Verlängerungen oder Harmonisierungen dürfen nur nach vorheriger Freigabe durch den Auftraggeber erfolgen.
- Die für die Angebotskalkulation verbindliche Prämisse zur Behandlung von Komponenten, deren Endkundenzuordnung beim Hersteller nicht auf den Auftraggeber lautet oder nicht feststellbar ist, ergibt sich aus Kapitel 20.2.

18 Service Level, Eskalation und Qualitätssicherung

18.1 Servicezeiten

Leistung	Servicezeit
Serviceannahme für kritische Incidents	24 Stunden an 7 Tagen pro Woche
Monitoring	24 Stunden an 7 Tagen pro Woche
P1-Bearbeitung	24 Stunden an 7 Tagen pro Woche
Regelbetrieb P2-P4	Gemäß Servicezeiten und Prioritätenmodell
Change-Durchführung	Nach abgestimmtem Wartungsfenster
Service Reviews	Regelmäßig nach Governance-Modell

Tabelle 24: Servicezeiten

18.2 SLA-Modell

Das SLA-Modell richtet sich nach der Auswirkung auf den Betrieb. Die Priorität bestimmt sich aus Impact, Dringlichkeit, betroffenen Bereichen, Redundanzsituation, Workaroundfähigkeit und klinischer Relevanz.

Die initiale Priorität wird durch den Auftraggeber oder nach definiertem Vorqualifizierungsprozess vergeben. Eine Herabstufung durch den Auftragnehmer ist nur nach Abstimmung und Dokumentation zulässig.

18.3 Eskalationsmatrix

Priorität	1. Eskalation	2. Eskalation	Weitere Eskalation
P1	Sofort bei Annahme	Nach 2 Stunden oder bei drohender Zielverfehlung	Alle 30 Minuten bzw. nach Lage
P2	Sofort bei kritischer Wirkung, sonst nach Prozess	Nach 2 Stunden bei drohender Zielverfehlung	Nach Lage und Impact
P3	Nach 4 Stunden bei fehlendem Fortschritt	Nach 24 Stunden	Alle 12 Stunden bei kritischer Entwicklung
P4	Nach Vereinbarung	Nach Vereinbarung	Nach Vereinbarung

Tabelle 25: Eskalationsmatrix

18.4 Qualitätssicherung

Der Auftragnehmer muss die Einhaltung der Servicequalität laufend überwachen und im Reporting nachweisen. SLA-Verletzungen sind zu begründen und mit Korrekturmaßnahmen zu versehen.

Wiederholte SLA-Verletzungen, unzureichende Dokumentation, mangelhafte Change-Qualität oder fehlende Reaktionsfähigkeit sind im Steering Committee zu behandeln.

18.5 Entschuldbare Leistungsminderungen

Leistungsminderungen sind nur entschuldbar, wenn sie außerhalb des Einflussbereichs des Auftragnehmers liegen, rechtzeitig angezeigt wurden und der Auftragnehmer alle zumutbaren Gegenmaßnahmen ergriffen hat.

Beispiele können fehlender Zutritt, fehlende Freigaben, ausgefallene Drittleistungen außerhalb der Verantwortung des Auftragnehmers oder vom Auftraggeber bewusst weiterbetriebene nicht supportete Komponenten sein. Die Entschuldigung wirkt nur für den konkret betroffenen Sachverhalt und nur soweit die Ursache tatsächlich kausal war.

18.6 Malus-Regelung bei SLA-Verletzungen

- Zur Sicherstellung der vereinbarten Servicequalität gelten bei erheblichen oder wiederholten Verletzungen der vereinbarten Service Level Malus-Regelungen. Die Malus-Regelungen dienen der vertraglichen Qualitätssicherung und entbinden den Auftragnehmer nicht von der Pflicht zur

unverzüglich die Wiederherstellung des ordnungsgemäßen Betriebs, zur Ursachenanalyse und zur Umsetzung geeigneter Verbesserungsmaßnahmen.

- Malus-relevant sind ausschließlich SLA-Verletzungen, die dem Verantwortungsbereich des Auftragnehmers zuzurechnen sind. Entschuldbare Leistungsminderungen gemäß Kapitel 18.5 bleiben unberührt.
- Maßgebliche Grundlage für die Bewertung sind die im führenden Ticketsystem des Auftraggebers dokumentierten Zeiten, Prioritäten, Bearbeitungsverläufe, Eskalationen und Abschlussinformationen. Eine nachträgliche Herabstufung von Prioritäten durch den Auftragnehmer ist nur nach Abstimmung mit dem Auftraggeber und nachvollziehbarer Dokumentation zulässig.

18.7 Malus bei Verletzung von Incident-SLAs

- Unabhängig von der technischen Verfügbarkeit führt die Überschreitung vereinbarter Reaktions- oder Wiederherstellungszeiten bei Incidents zu einem Malus, sofern die Überschreitung durch den Auftragnehmer zu vertreten ist.
- Der Malus wird auf das monatliche Serviceentgelt der jeweils betroffenen Servicekategorie angewendet. Betroffen ist diejenige Servicekategorie, der der gestörte Netzbereich, Standort, Porttyp oder Servicebestandteil zugeordnet ist.

Priorität	Malus bei zurechenbarer SLA-Verletzung
P1 / Kritisch	5,0 % des betroffenen monatlichen Serviceentgelts je Ereignis
P2 / Hoch	2,5 % des betroffenen monatlichen Serviceentgelts je Ereignis
P3 / Mittel	0,5 % des betroffenen monatlichen Serviceentgelts je Ereignis
P4 / Niedrig	kein automatischer Malus, aber Berücksichtigung im Qualitätsreporting

- Mehrere zurechenbare SLA-Verletzungen innerhalb eines Kalendermonats können addiert werden, bleiben jedoch der Deckelung gemäß Kapitel 18.11 unterworfen.

18.8 Malus bei wiederholten Verfügbarkeitsverletzungen

- Werden die vereinbarten Verfügbarkeitsziele einer Servicekategorie innerhalb eines Kalendermonats unterschritten und ist die Unterschreitung durch den Auftragnehmer zu vertreten, kann ein abgestufter Malus auf das monatliche Serviceentgelt der betroffenen Servicekategorie angewendet werden.
- Maßgeblich sind die in diesem Leistungsverzeichnis bzw. in den Vertragsunterlagen festgelegten Zielwerte je Servicekategorie. Eine pauschale Anwendung einheitlicher Verfügbarkeitswerte auf alle Netzbereiche erfolgt nicht.

Abweichung vom vereinbarten Verfügbarkeitsziel	Malus
geringfügige Unterschreitung	2,5 % des betroffenen monatlichen Serviceentgelts
erhebliche Unterschreitung	5,0 % des betroffenen monatlichen Serviceentgelts
schwerwiegende Unterschreitung	10,0 % des betroffenen monatlichen Serviceentgelts

- Die konkrete Zuordnung zu geringfügiger, erheblicher oder schwerwiegender Unterschreitung erfolgt anhand der vereinbarten SLA-Zielwerte, der Dauer der Beeinträchtigung, der betroffenen Redundanzsituation und der klinischen Auswirkung.
- Dieselbe Ursache darf nicht doppelt als Verfügbarkeitsmalus und Incident-Malus bewertet werden, soweit dadurch dieselbe Leistungsminderung mehrfach sanktioniert würde. In diesem Fall ist der für den Auftragnehmer günstigere Malus anzuwenden. Die Kumulierung mehrerer Malus-Ansprüche (Verfügbarkeits-Malus, Incident-Malus, Prozess-Malus) für denselben Leistungsbereich im selben Abrechnungszeitraum ist ausgeschlossen; je Leistungsbereich und Abrechnungszeitraum findet nur ein Malus-Anspruch Anwendung.

18.9 Malus bei Prozess- und Dokumentationsverletzungen

- Ergänzend zu Incident- und Verfügbarkeits-SLAs werden wesentliche Prozessqualitäten überwacht. Hierzu zählen insbesondere:
- fristgerechte Ticketannahme und Statuspflege,

- vollständige Ticketdokumentation,
- termingerechte Durchführung freigegebener Changes,
- fristgerechte Bereitstellung vereinbarter Reports,
- Aktualisierung von CMDB, Betriebshandbuch und Betriebsdokumentation,
- Einhaltung vereinbarter Eskalations- und Kommunikationswege.
- Werden vereinbarte Prozesskennzahlen wiederholt oder erheblich verletzt, kann der Auftraggeber eine Minderung des betroffenen Leistungsanteils geltend machen. Dies gilt insbesondere, wenn mangelhafte Dokumentation, fehlende Statuspflege oder verspätete Eskalation die Steuerungsfähigkeit des Auftraggebers beeinträchtigen.
- Werden mehr als 5 % der im jeweiligen Kalendermonat fälligen und freigegebenen Changes ohne abgestimmte Verschiebung nicht termingerecht durchgeführt oder nicht ordnungsgemäß dokumentiert, kann der auf Change- und Release-Management entfallende Leistungsanteil um 10 % gemindert werden. Für weitere gleichartige Überschreitungen kann eine zusätzliche Minderung um jeweils 5 % erfolgen.

18.10 Reporting und Messung

- Der Auftragnehmer stellt dem Auftraggeber monatlich einen SLA-Bericht zur Verfügung, der alle für die Malus-Berechnung relevanten Kennzahlen enthält. Der Bericht ist spätestens am 5. Werktag des Folgemonats in der vereinbarten Form zu übermitteln.
- Der Bericht enthält mindestens:
- Verfügbarkeitswerte je Leistungsbereich (Ist vs. Zielwert),
- Incidents nach Priorität und Lösungszeit,
- Anzahl und Status offener sowie abgeschlossener Changes,
- Prozesskennzahlen (Ticketdokumentation, Statuspflege, Eskalationen),
- Berechnung etwaiger Malus-Beträge inkl. Herleitung.
- Beide Parteien benennen jeweils einen SLA-Verantwortlichen, der für die Prüfung der Berichte und die Abwicklung etwaiger Malus-Abzüge zuständig ist. Einwendungen gegen den Bericht sind innerhalb von 10 Werktagen nach Übermittlung schriftlich mitzuteilen; anderenfalls gilt der Bericht als anerkannt.
- Malus-Abzüge werden mit der auf den Berichtsmonat folgenden Abrechnung verrechnet, sofern keine abweichende Vereinbarung getroffen wurde.

18.11 Deckelung der Malus-Beträge

- Die Summe der in einem Kalendermonat je Servicekategorie anfallenden Malus-Beträge (Incident-Malus nach Kapitel 18.7, Verfügbarkeits-Malus nach Kapitel 18.8 und Prozess- und Dokumentations-Malus nach Kapitel 18.9) ist auf höchstens 12 % des auf die betroffene Servicekategorie entfallenden monatlichen Serviceentgelts begrenzt. Die Deckelung lässt die Pflicht des Auftragnehmers zur unverzüglichen Wiederherstellung des ordnungsgemäßen Betriebs, zur Ursachenanalyse und zur Mängelbeseitigung sowie sonstige vertragliche Rechte des Auftraggebers, insbesondere Kündigungs- und Schadensersatzrechte, unberührt.

19 Betriebsorganisation, Rollen und Governance

19.1 Rollen des Auftragnehmers

Rolle	Aufgaben
Service Delivery Manager	Zentrale Schnittstelle, Servicequalität, Reporting, Eskalation, Governance
Technischer Betriebsverantwortlicher Netzwerk	Technische Steuerung, Architekturbezug, Betriebsstandards
Incident Manager	Qualität und Steuerung des Incident-Prozesses
Problem Manager	Ursachenanalyse, Known Errors, Trends und Prävention
Change Manager	Planung, Bewertung, Freigabevorbereitung und Nachbereitung von Changes
Release-/Lifecycle-Verantwortlicher	Firmware, Advisories, EoL/EoS und Updateplanung
Security-Ansprechpartner	Schnittstelle zu ISB, SOC/SIEM und Security Incidents
Dokumentationsverantwortlicher	Betriebshandbuch, Knowledge Base, CMDB-Qualität

Tabelle 26: Rollen des Auftragnehmers

19.2 Qualifikationsanforderungen

Der Auftragnehmer muss ein qualifiziertes Team bereitstellen, das die bestehende Cisco-Infrastruktur fachlich beherrscht. Die Qualifikation muss nicht nur durch Zertifikate, sondern auch durch praktische Erfahrung in vergleichbaren Enterprise-Umgebungen nachgewiesen werden.

Der Auftraggeber erwartet ausreichend verfügbare Ressourcen für 2nd- und 3rd-Level-Aufgaben. Kritische Störungen dürfen nicht davon abhängen, dass nur einzelne Personen beim Auftragnehmer über notwendiges Wissen verfügen.

- Nachweis praktischer Erfahrung im Cisco Enterprise Switching und Routing.
- Nachweis praktischer Erfahrung im Cisco WLAN-Betrieb und Controllerumfeld.
- Erfahrung mit Netzwerk-Monitoring und ITSM-Integration.
- Erfahrung mit Change- und Release-Prozessen in produktiven KRITIS- oder vergleichbaren Umgebungen.
- Erfahrung mit NAC-/AAA-Schnittstellen und segmentierten Netzwerkumgebungen.
- Benennung von Vertretungen für Schlüsselrollen.

19.3 Meetingstruktur

Termin	Frequenz	Inhalt
SOT Daily / Kurzabstimmung	Während SOT nach Bedarf, bei kritischer Lage täglich	Fortschritt, Risiken, Zugänge, offene Punkte
Operational Service Review	Monatlich	Tickets, SLA, Changes, Problems, Risiken, Maßnahmen
Technisches Betriebsmeeting	Monatlich oder nach Bedarf	Architektur, Standards, Lifecycle, Modernisierung
Steering Committee	Quartalsweise	Managementsicht, Eskalationen, Roadmap, Budget-/Leistungsthemen
Major-Incident-Review	Anlassbezogen	RCA, Maßnahmen, Lessons Learned
Exit-Meeting	Ab sechs Monate vor Vertragsende regelmäßig	Übergabepanung, Nachweise, offene Risiken

Tabelle 27: Meetingstruktur

19.4 Ressourcen- und Fluktuationsmanagement

Der Auftragnehmer muss sicherstellen, dass Personalwechsel, Krankheit, Urlaub oder Fluktuation nicht zu einer Leistungsminderung führen. Schlüsselrollen dürfen nicht ohne geordnete Übergabe ausgetauscht werden.

Bei Wechseln sind Wissenstransfer, Aktualisierung der Dokumentation und Übergabe offener Themen sicherzustellen. Aufwände aus normaler Fluktuation trägt der Auftragnehmer.

20 Kalkulations- und Abrechnungsmodell

20.1 Grundsatz

Das Kalkulations- und Abrechnungsmodell dient der transparenten Abbildung der laufenden Managed-Service-Leistungen sowie der separat ausgewiesenen einmaligen Leistungen gemäß Preismatrix.

Die laufenden Managed-Service-Leistungen werden über definierte Port- bzw. Serviceeinheiten abgebildet. Der Auftragnehmer hat seine Einheitspreise so zu kalkulieren, dass der laufende Betrieb, die Entstörung, die betriebliche Pflege, die Dokumentation, die Überwachung sowie die betriebliche Einbindung ersetzter oder ausgetauschter Komponenten im vereinbarten Umfang enthalten sind.

Einmalige Projekt-, Zielbild-, Design-, Transformations- oder Überführungsleistungen sind nur dann gesondert abrechenbar, wenn sie in der Preismatrix ausdrücklich als eigene Leistungsposition ausgewiesen sind.

Eine doppelte Abrechnung derselben Komponente, desselben Ports oder desselben Netzbereichs ist ausgeschlossen.

20.2 Preisbestandteile

Die Preismatrix unterscheidet die nachfolgend dargestellten Preisbestandteile.

Preisbestandteil	Beschreibung	Abrechnungsform
Service Ownership Transfer	Due Diligence, Betriebsübernahme, Toolanbindung, initiale Betriebsdokumentation	Einmaliger Festpreis
Zielbild- und Designleistungen	Stabilisierung, Bewertung, Zielbild, Design, Konzept- und Planungsleistungen, soweit in der Preismatrix als eigene Position ausgewiesen	Einmaliger Festpreis bzw. Position gemäß Preismatrix
Überführung in das Zielbetriebsmodell	Einmalige Überführung von Netzbereichen, Komponentengruppen oder größeren Portmengen in das freigegebene Ziel- und Betriebsdesign	Einmalige Position gemäß Preismatrix
Laufender Managed Service CMO	Laufender Betrieb der bestehenden Infrastruktur gemäß den Betriebskapiteln	Einheitspreis pro Port-Einheit, Quartal und Servicequalität CMO
Laufender Managed Service FMO	Laufender Betrieb von Ports, Komponenten oder Netzbereichen, die formal in den Zielbetrieb übernommen wurden	Einheitspreis pro Port-Einheit, Quartal und Servicequalität FMO
Exit- und Providerwechselunterstützung	Datenexport, Dokumentation, Knowledge Transfer, Unterstützung bei Providerwechsel, soweit in der Preismatrix gesondert ausgewiesen	Position gemäß Preismatrix
Sachsenhausen	Zeitversetzter Leistungsumfang Sachsenhausen mit separater Mengen- und Wertungssystematik	Identische Einheitspreise, separates Mengengerüst gemäß Preismatrix
Einmalige Installations- und Einbindungsleistungen WLAN-Access-Points	Die laufende Betriebsleistung für die zusätzlich installierten WLAN-Access-Points ist in den FMO-Leistungen enthalten. Separat zu kalkulieren sind lediglich einmalige Installations-, Montage- und Einbindungsleistungen, sofern diese nicht bereits über bestehende Integrationspositionen der Preismatrix abgedeckt sind.	Pro AP gemäß Preismatrix
Nachausleuchtung / WLAN-Survey (optional)	Nachausleuchtungen bzw. WLAN-Surveys sind als optionale einmalige Leistung gemäß Preismatrix abzubilden, sofern sie nicht Bestandteil der jeweiligen	Optionale einmalige Position gemäß Preismatrix

Preisbestandteil	Beschreibung	Abrechnungsform
	Installations- oder Integrationsleistung sind.	
Herstellerbezogener Software-Support / Bugfixes / Updates	Leistungen zur Prüfung, Koordination und optionalen Einbuchung eines herstellerbezogenen Software-Supports für im Scope befindliche Bestandskomponenten. Die tatsächliche Supportfähigkeit und die herstellerseitigen Kosten können erst nach Bereitstellung vollständiger Asset- und Seriennummerninformationen verbindlich festgestellt werden. Herstellkosten werden nur nach Freigabe durch den Auftraggeber und gegen Nachweis berücksichtigt.	Gesonderte Position gemäß Preisblatt; Abrechnung nach tatsächlich beauftragtem und nachgewiesenem Herstellersupport

Tabelle 28: Preisbestandteile

Herstellkosten für Software-, Subscription-, Bugfix-, Update- oder Security-Advisory-Ansprüche werden nur nach vorheriger Freigabe des Auftraggebers und gegen prüffähigen Nachweis berücksichtigt. Hardwaretausch, Ersatzteilbereitstellung, Vor-Ort-Austausch, Hardwarelieferungen und pauschale RMA-Leistungen sind nicht Bestandteil dieser Position.

Klarstellung zur Kalkulation des herstellerbezogenen Software-Supports: Der in Anlage P anzugebende Einheitspreis je Gerät umfasst ausschließlich die eigenen Prüf-, Koordinations- und Administrationsleistungen des Auftragnehmers. Herstellerseitige Fremdkosten – insbesondere Distributor-/Reseller-, Subscription-, Lizenz-, Reinstatement-, Nachregistrierungs-, Co-Termin- und Übertragungskosten, z. B. bei einem Mid-Term-Takeover – sind nicht im Einheitspreis enthalten. Sie werden ausschließlich nach vorheriger schriftlicher Freigabe des Auftraggebers und gegen prüffähigen Nachweis ohne pauschalen Aufschlag vergütet.

Für Komponenten, deren Cisco-Endkundenzuordnung zum Zeitpunkt der Angebotsabgabe nicht auf das Universitätsklinikum Frankfurt lautet oder nicht feststellbar ist, sind für die Angebotswertung unverändert die im Blatt „Software-Support“ vorgegebenen Mengen und Laufzeiten anzusetzen. Die Komponenten sind für die Kalkulation des Einheitspreises als grundsätzlich supportfähig zu behandeln; die verbindliche Prüfung der Endkundenzuordnung, vorhandener Entitlements, bestehender Service-Coverage und der tatsächlichen Supportfähigkeit erfolgt in der SOT-Phase. Ergibt die Prüfung, dass herstellerbezogener Software-Support nicht verfügbar ist, gelten für die betreffende Komponente die Regelungen nach Kapitel 17.5. Hieraus entstehende herstellerseitige Reinstatement-, Nachregistrierungs- oder Übertragungskosten sind nicht im Einheitspreis enthalten und unterliegen dem vorstehenden Freigabe- und Nachweismechanismus. Bei der Übertragung bestehender Cisco-Service-Coverage stellt der Auftraggeber die verfügbaren Vertrags- und Seriennummerninformationen bereit und leitet die erforderliche Service Cancellation ein.

Eine unzutreffende, unvollständige oder nicht auf den Auftraggeber lautende Endkundenregistrierung von Bestandskomponenten hat der Auftragnehmer nicht zu vertreten. Hieraus resultierende Mehrkosten oder Verzögerungen begründen kein Haftungs- oder Kostenrisiko des Auftragnehmers; sie werden ausschließlich über den vorstehenden Freigabe- und Nachweismechanismus behandelt. Die Service-Level-Folgen richten sich nach Kapitel 17.5 in Verbindung mit Kapitel 18.5.

Der reguläre Austausch, die betriebliche Wiederinbetriebnahme und die Einbindung einzelner Ersatzkomponenten in den bestehenden CMO- oder FMO-Betrieb sind Bestandteil der laufenden Managed-Service-Leistung, soweit es sich nicht um eine in der Preismatrix gesondert ausgewiesene Überführung eines Netzbereichs in das Zielbetriebsmodell handelt.

Hardwarelieferungen, Lizenzen, Subscriptions, Herstellerwartungen und passive Infrastrukturmaßnahmen sind nicht Bestandteil der laufenden Port-Servicepauschalen, sofern sie nicht ausdrücklich gesondert beauftragt werden.

Zur kalkulatorischen Vergleichbarkeit sind in der Preismatrix optionale Erweiterungsszenarien für zusätzliche WLAN-Access-Points vorzusehen. Hierfür sind mindestens zwei Mengenszenarien abzubilden: Integration

und Betriebsübernahme von zusätzlich ca. 1.500 WLAN-Access-Points sowie Integration und Betriebsübernahme von zusätzlich ca. 2.000 WLAN-Access-Points.

20.3 Port-Kategorien

Für die laufenden Managed-Service-Leistungen werden drei Port- bzw. Servicekategorien unterschieden.

- **Managed LAN Access Port:** Physischer aktiver Access-Port zur Anbindung produktiver Endpunkte wie Arbeitsplatzgeräte, Medizintechnik, IoT-Geräte, Drucker, Telefone oder sonstige Anschlussobjekte.
- **Managed DC- bzw. Distribution-Port:** Physischer Port im Rechenzentrum, Core-, Backbone-, Distribution-, Aggregations- oder Uplink-Bereich, einschließlich Top-of-Rack- und Serveranbindungen, Gebäude-Uplinks, Trunks, redundanter Verbindungen und zentraler Übergabepunkte.
- **Managed WLAN Service Point:** Ein Access Point als logische Serviceeinheit. Die Abrechnung erfolgt je Access Point, unabhängig vom konkreten Modell, sofern die Preismatrix keine abweichende Differenzierung vorsieht.

Zentrale Betriebsanteile wie NOC- bzw. Service-Desk-Betrieb, Monitoring, Tooling, ITSM-Prozessbetrieb, Dokumentationspflege, Reporting, Eskalation und Governance sind sachgerecht in die Einheitspreise einzukalkulieren. Sie dürfen nicht zusätzlich als nicht in der Preismatrix vorgesehene Pauschalen berechnet werden.

20.4 CMO-/FMO-Abgrenzung

Für die laufende Abrechnung werden zwei Servicequalitäten unterschieden.

- **CMO – Current Mode of Operation:** Betrieb der bestehenden Infrastruktur im aktuellen Betriebsmodus. Dies umfasst insbesondere den Betrieb der vorhandenen Bestandsarchitektur mit bestehenden Komponenten, Softwareständen, Sonderkonfigurationen, manuellen Betriebsanteilen und historisch gewachsenen Betriebsmechanismen.
- **FMO – Future Mode of Operation:** Betrieb von Ports, Komponenten oder Netzbereichen, die nach dem in der Zielbild-, Design- oder Überführungsphase freigegebenen Zielzustand technisch umgesetzt, dokumentiert, getestet und formal in den Zielbetrieb übernommen wurden.

Ein Port, eine Komponente oder ein Netzbereich gilt erst dann als FMO, wenn das für diesen Bereich definierte Zielbild bzw. Design umgesetzt wurde. Maßgeblich ist nicht allein der Austausch einer Komponente, sondern die vollständige Überführung in das definierte technische Design und Betriebsmodell.

Zur FMO-Zuordnung müssen mindestens folgende Voraussetzungen erfüllt sein:

- das Zielbild bzw. technische Design für den betreffenden Bereich wurde durch den Auftraggeber freigegeben;
- die technische Umsetzung erfolgte gemäß dem freigegebenen Zielbild bzw. Design;
- die vorgesehenen Portprofile, Betriebsprofile, VLAN-/Segmentierungs-/Policy-Vorgaben oder vergleichbaren Zielvorgaben sind umgesetzt;
- die Komponente bzw. der Portbereich ist in die vorgesehene Management-, Monitoring- und Betriebsumgebung eingebunden;
- CMDB-, Asset- und Portdokumentation sind gepflegt;
- Konfigurationssicherung ist eingerichtet;
- Betriebs- und Supportzuständigkeiten sind dokumentiert;
- Funktions-, Integrations- oder Abnahmetests wurden erfolgreich durchgeführt;
- die formale Betriebsübernahme durch den Auftraggeber ist erfolgt.

Bis zur Erfüllung dieser Kriterien verbleibt der jeweilige Port, die Komponente oder der Netzbereich abrechnungstechnisch im CMO oder wird, sofern noch nicht in den Managed Service übernommen, nicht als laufende FMO-Leistung abgerechnet.

Eine doppelte Abrechnung desselben Ports, derselben Komponente oder desselben Netzbereichs als CMO und FMO ist ausgeschlossen.

20.5 Abgrenzung zwischen laufendem Betrieb und Überführung in das Zielbetriebsmodell

Der laufende CMO- bzw. FMO-Betrieb umfasst die betriebliche Betreuung, Entstörung, Überwachung, Dokumentation und Pflege der im Managed Service befindlichen Ports, Komponenten und Netzbereiche gemäß den Regelungen dieses Leistungsverzeichnisses.

Die laufenden Managed-Service-Leistungen werden über die CMO-/FMO-Portpauschalen vergütet. Hierzu gehören insbesondere die in Kapitel 20.6 beschriebenen Betriebsleistungen, einschließlich Incident Management, Service Request Management, Standard- und Minor-Changes, Problem Management, Configuration Management, Monitoring, Reporting, RMA-/Herstellerkoordination im beschriebenen Umfang sowie die betriebliche Einbindung einzelner gleichartiger Ersatzkomponenten in den bestehenden Betriebszustand.

-

Nicht über die laufenden CMO-/FMO-Portpauschalen abgegolten sind einmalige TMO-Überführungsleistungen, soweit diese in der Preismatrix ausdrücklich als eigene Leistungspositionen ausgewiesen sind. Hierzu zählt die strukturierte Überführung eines Netzbereichs, einer Komponentengruppe oder größerer Portmengen aus dem bestehenden CMO-/Legacy-Betrieb in ein freigegebenes Ziel- und Betriebsdesign.

Hierzu zählen insbesondere:

-

Eine gesonderte Vergütung als TMO-Leistung setzt voraus, dass die Leistung in der Preismatrix vorgesehen, durch den Auftraggeber freigegeben und nicht bereits Bestandteil der laufenden CMO-/FMO-Portpauschalen ist. Eine doppelte Abrechnung derselben Leistung über Portpauschale und TMO-Position ist ausgeschlossen.

Die konkrete Zuordnung eines Netzbereichs zum FMO erfolgt erst nach erfolgreicher Umsetzung, Dokumentation, Test und formaler Abnahme gemäß den Regelungen dieses Leistungsverzeichnisses. Bis dahin verbleibt der betreffende Netzbereich abrechnungstechnisch im CMO bzw. im zuletzt freigegebenen Betriebszustand.

20.6 Zuordnung der Port-Pauschale zu den Managed-Service-Leistungen

Der Port-Preis bildet die laufenden Managed-Service-Leistungen für die jeweilige Port- bzw. Servicekategorie kaufmännisch ab.

Der Port-Preis umfasst insbesondere:

- Incident Management einschließlich Entstörung, Koordination und Dokumentation;
- Service Request Management für definierte Standardanforderungen;
- Change Management für Standard- und Minor-Changes im vereinbarten Umfang;
- Problem Management einschließlich Ursachenanalyse und Trendbewertung;
- Configuration Management einschließlich CMDB-, Asset- und Portpflege;
- Monitoring, Alarmierung und Betriebsüberwachung;
- SLA-Steuerung, Eskalation und Reporting;
- RMA- und Herstellerkoordination im beschriebenen Umfang, ohne Hardware- oder Herstellerwartungskosten;
- betriebliche Einbindung ersetzter oder ausgetauschter Einzelkomponenten in den bestehenden CMO- oder FMO-Betrieb;
- Pflege der betriebsrelevanten Dokumentation;
- Sicherheitsbetrieb gemäß Kap. 15 einschließlich Erkennung, Bewertung und Meldung sicherheitsrelevanter Netzwerkeignisse an die definierten Sicherheitsrollen des Auftraggebers.

Nicht über den Port-Preis abgegolten sind:

- Service-Ownership-Transfer- und Transitionsleistungen, soweit in der Preismatrix separat ausgewiesen;
- Zielbild-, Design- und Konzeptleistungen, soweit in der Preismatrix separat ausgewiesen;

- einmalige Überführungsleistungen in das Zielbetriebsmodell gemäß Kap. 20.5, soweit in der Preismatrix separat ausgewiesen;
- Hardwarelieferungen;
- Lizenzen, Subscriptions und Herstellerwartung;
- passive Infrastrukturmaßnahmen.

20.7 Zähl- und Abrechnungsregeln

Ein Port bzw. eine Serviceeinheit ist abrechnungsrelevant, wenn folgende Voraussetzungen kumulativ erfüllt sind:

- er bzw. sie wird produktiv genutzt oder ist einem produktiven Service zugeordnet;
- er bzw. sie ist administrativ aktiv;
- er bzw. sie liegt im Managed-Service-Scope;
- er bzw. sie ist in CMDB, Asset- oder Portdokumentation geführt.

Für die Zählung gelten folgende Regeln:

- Managed LAN Access Port: je physischem produktiv genutztem Edge-Port eine Einheit;
- Managed WLAN Service Point: je Access Point eine Einheit;
- Managed DC- bzw. Distribution-Port: je physischem produktiv genutztem Link-, Uplink- oder Trunk-Port eine Einheit;
- Link Aggregation: Mitgliedsports zählen einzeln;
- Reserve- und Dark-Ports: nicht abrechnungsrelevant, solange sie nicht produktiv genutzt werden;
- Out-of-Band-Managementports: nicht abrechnungsrelevant, sofern sie ausschließlich für Management genutzt werden;
- interne Backplane- bzw. Chassis-Verbindungen: nicht abrechnungsrelevant, sofern kein produktiver Serviceübergabepunkt besteht.

Mengenänderungen sind gemäß Preismatrix und abgestimmter Bestandsdokumentation nachzuführen. Grundlage des quartalsweisen Abgleichs sind die CMDB- bzw. Bestandsdaten. Die abrechnungsrelevante Quartalsmenge ergibt sich aus dem Mittelwert der monatlichen Bestands-Snapshots des jeweiligen Quartals. Der Abgleich wird zwischen Auftraggeber und Auftragnehmer protokolliert und vom Auftraggeber freigegeben.

Sachsenhausen ist separat gemäß Preismatrix zu behandeln und erst ab dem dort vorgesehenen Zeitpunkt bzw. ab formaler Betriebsübernahme in die laufende Servicevergütung einzubeziehen. Die Einheitspreise je Port-Kategorie und Servicequalität gelten für Sachsenhausen identisch.

Die Einheitspreise sind für die Vertragslaufzeit verbindlich. Preisanpassungen sind nur zulässig, soweit dies im Vertrag ausdrücklich geregelt ist. Rückwirkende Nachforderungen aufgrund unzureichender Bestandsprüfung sind ausgeschlossen, soweit die relevanten Informationen dem Auftragnehmer vor Angebotsabgabe oder im Rahmen des Service Ownership Transfers zugänglich waren und keine abweichende Vereinbarung getroffen wurde.

21 Anforderungen an einzureichende Konzepte

21.1 Projekt-, Transition- und Betriebsübernahmekonzept

Der Bieter hat ein Konzept vorzulegen, wie er die bestehende Cisco-Infrastruktur sicher übernimmt und in den Managed Service überführt. Das Konzept muss realistische Ressourcen, Meilensteine, Risiken und Abnahmekriterien enthalten.

- Vorgehen für SOT und Due Diligence.
- Umgang mit fehlender oder widersprüchlicher Dokumentation.
- Einrichtung administrativer Zugänge.
- Integration in ServiceNow und Monitoring.
- Aufbau des Betriebshandbuchs.

- Risikomanagement während der Übernahme.
- Abnahmekriterien und SLA-Start.

21.2 Managed-Service- und Betriebskonzept

Der Bieter muss sein Betriebsmodell für den Regelbetrieb beschreiben. Dabei ist insbesondere darzustellen, wie qualifizierte Cisco-Betriebsfähigkeit, NOC-/Service-Desk-Leistungen, Eskalationen und 24/7-Fähigkeit für kritische Incidents sichergestellt werden.

- NOC-/Service-Desk-Modell.
- 2nd-/3rd-Level-Struktur.
- Rollen und Vertretungen.
- Incident-, Problem-, Change- und Release-Prozesse.
- Monitoring- und Eventkorrelation.
- Reporting und Service Reviews.
- Knowledge Management und Dokumentationspflege.

21.3 Zielbild-, Standardisierungs- und Automatisierungskonzept

Der Bieter muss darstellen, wie der Betrieb der heutigen Infrastruktur schrittweise in Richtung eines standardisierten, automatisierten und besser dokumentierten Zielbetriebs entwickelt werden kann. Das Konzept muss die Schnittstelle zu separat beschaffter Hardware berücksichtigen.

- Bewertung der bestehenden Architektur.
- Vorschlag für Standardisierung und Betriebsprofile.
- Automatisierungsansatz für wiederkehrende Betriebsaufgaben.
- Messgrößen für Standardisierung und Automatisierung.
- Integrationsvorgehen für bereitgestellte Komponenten.
- Abhängigkeiten und Risiken.

21.4 Lifecycle- und Risikomanagementkonzept

Der Bieter muss beschreiben, wie EoL-/EoS-Risiken, Security Advisories, Ersatzteilrisiken und Softwarestände überwacht, bewertet und berichtet werden. Das Konzept muss zeigen, wie Risiken priorisiert und in Maßnahmen überführt werden.

21.5 Exit- und Providerwechselkonzept

Der Bieter muss darstellen, wie er die geordnete Übergabe am Vertragsende oder bei vorzeitiger Vertragsbeendigung sicherstellt. Das Konzept muss nicht nur die letzten Vertragsmonate beschreiben, sondern auch die laufende Sicherstellung der Providerwechselfähigkeit.

22 Abnahmen, Nachweise und Vertragssteuerung

22.1 Abnahmearten

Im Rahmen dieses Leistungsverzeichnisses sind mehrere Abnahmen erforderlich. Sie dienen dazu, Leistungsstände eindeutig festzustellen und spätere Unklarheiten zu vermeiden.

Abnahme	Gegenstand	Mindestnachweis
SOT-Abnahme	Betriebsübernahme und SLA-Startfähigkeit	Due-Diligence-Bericht, Betriebshandbuch, Monitoring, ITSM-Test
Konzeptabnahme	Zielbild- und Umsetzungskonzept	Freigegebenes Konzept mit Meilensteinen und Risiken
Integrationsabnahme	Übernahme eines Netzbereichs oder einer Komponente	Funktionstest, CMDB, Monitoring, Dokumentation
Betriebsabnahme FMO	Überführung eines Bereichs in Zielbetrieb	Nachweis Servicefähigkeit und Standardisierung
Exit-Abnahme	Vollständige Übergabe	Übergabeprotokoll und Daten-/Dokumentationsnachweise

Tabelle 29: Abnahmearten

22.2 Nachweispflichten

Der Auftragnehmer muss alle wesentlichen Leistungen nachvollziehbar nachweisen. Nachweise müssen so geführt werden, dass der Auftraggeber die Leistung prüfen und bei Bedarf gegenüber internen oder externen Prüfern darlegen kann.

- Service Reports.
- Ticket- und SLA-Auswertungen.
- Change-Dokumentationen.
- Root-Cause-Analysen.
- CMDB- und Asset-Reports.
- Lifecycle- und EoL-/EoS-Register.
- Betriebshandbuch-Versionen.
- Konfigurationssicherungsnachweise.
- Abnahmeprotokolle.

22.3 Vertragssteuerung

Die Vertragssteuerung erfolgt über Regelmeetings, Service Reports, Eskalationswege und formale Abnahmen. Der Auftragnehmer muss Abweichungen frühzeitig anzeigen und darf kritische Risiken nicht bis zum nächsten Regeltermin zurückhalten.

Der Auftraggeber behält sich vor, bei wiederholten Qualitätsmängeln Sondertermine, Maßnahmenpläne oder Managementeskalationen zu verlangen.

23 Exit Management

23.1 Ziel

Das Exit Management stellt sicher, dass der Auftraggeber den Netzbetrieb am Ende der Vertragslaufzeit oder bei vorzeitiger Beendigung geordnet an einen Nachfolgeprovider oder in eine Eigenbetriebsorganisation überführen kann.

Der Auftragnehmer muss vermeiden, dass betriebsrelevantes Wissen ausschließlich in nicht übergabefähigen internen Systemen, persönlichen Notizen oder nicht exportierbaren Werkzeugen verbleibt.

23.2 Laufende Exit-Fähigkeit

Providerwechselfähigkeit ist während der gesamten Vertragslaufzeit sicherzustellen. Der Auftragnehmer muss Dokumentation, Konfigurationen, CMDB-Daten, Runbooks und Known Errors laufend so führen, dass eine Übergabe mit angemessenem Aufwand möglich ist.

23.3 Formale Exit-Phase

Spätestens sechs Monate vor Vertragsende beginnt die formale Exit-Phase. Der Auftragnehmer erstellt einen Exit-Plan und stimmt diesen mit dem Auftraggeber ab.

Der Exit-Plan muss Zeitplan, Übergabeobjekte, Rollen, Datenexporte, Workshops, offene Risiken, Parallelbetriebsregelungen und Abschlusskriterien enthalten.

23.4 Übergabeobjekte

- Aktuelles Betriebshandbuch.
- Vollständige Netzwerkdokumentation im vereinbarten Umfang.
- CMDB-/Asset-Export.
- Konfigurationssicherungen und Versionsinformationen.
- Monitoring- und Alarmierungslogik.
- Known-Error-Database-Auszug.
- Offene Incidents, Problems, Changes und Risiken.
- Lifecycle- und EoL-/EoS-Übersicht.
- Service Reports und SLA-Historie.
- Zugriffs- und Berechtigungsdokumentation.
- Runbooks, SOPs und technische Betriebsanweisungen.

23.5 Unterstützung des Nachfolgeproviders

Der Auftragnehmer muss einen Nachfolgeprovider angemessen unterstützen. Dazu gehören Übergabeworkshops, Erläuterung der Betriebsdokumentation, Klärung offener technischer Fragen, Unterstützung bei Testzugriffen und Abstimmung offener Risiken.

Die Unterstützung erfolgt im Umfang der vertraglich festgelegten Exit-Leistung. Darüberhinausgehende Leistungen können gesondert beauftragt werden.

23.6 Rückgabe und Löschung

Nach Abschluss der Übergabe muss der Auftragnehmer Daten des Auftraggebers zurückgeben oder löschen, sofern keine gesetzlichen oder vertraglichen Aufbewahrungspflichten bestehen. Die Löschung ist nachvollziehbar zu bestätigen.

LEISTUNGSVERZEICHNIS

Ausschreibung (Korrektur 6)

12.08.2026

Verfahren: 20261019 - Netzbetrieb Managed Service

SKONTO

Skonto zugelassen	Nein
Zahlungsziel (falls zugelassen)	Tag(e)
Skonto	_____ %

AUFLISTUNG ALLER POSITIONEN

ALLE PREISE SIND OHNE UMSATZSTEUER ANZUGEBEN

1	Einmalpreis SOT – Service Ownership Transfer	USt. [%]	Menge	Einheit	Einzelpreis [EUR]	Gesamtpreis [EUR]
		19%	1,00	---	 pro 1,00 ---	

Bitte übertragen Sie den Preis aus Anlage P - Preismatrix; Deckblatt Zeile 38

2	Managed Service CMO + FMO (Wertung 60 Monate)	USt. [%]	Menge	Einheit	Einzelpreis [EUR]	Gesamtpreis [EUR]
		19%	1,00	---	 pro 1,00 ---	

Bitte übertragen Sie den Preis aus Anlage P - Preismatrix; Deckblatt Zeile 39

3	Einmalpreis TMO – Transition / Modernisierung inkl. Exit	USt. [%]	Menge	Einheit	Einzelpreis [EUR]	Gesamtpreis [EUR]
		19%	1,00	---	 pro 1,00 ---	

Bitte übertragen Sie den Preis aus Anlage P - Preismatrix; Deckblatt Zeile 40

4	Einmalpreis Überführung in das Zielbetriebsmodell	USt. [%]	Menge	Einheit	Einzelpreis [EUR]	Gesamtpreis [EUR]
		19%	1,00	---	 pro 1,00 ---	

Bitte übertragen Sie den Preis aus Anlage P - Preismatrix; Deckblatt Zeile 41

5	Herstellerbezogener Software-Support / Bugfixes / Updates (Wertung)	USt. [%]	Menge	Einheit	Einzelpreis [EUR]	Gesamtpreis [EUR]
		19%	1,00	---	 pro 1,00 ---	

Bitte übertragen Sie den Preis aus Anlage P - Preismatrix; Deckblatt Zeile 42

6	optionale Leistungen	USt. [%]	Menge	Einheit	Einzelpreis [EUR]	Gesamtpreis [EUR]
	Optionalposition	19%	1,00	---	 pro 1,00 ---	

Bitte tragen Sie die Zwischensumme aus Zeile 17 vom Blatt "optionale Leistungen" aus der Anlage P ein.

ANGEBOTSSUMME(N)

Summe exkl. Nachlass (netto)		
Nachlass (netto)		
Summe inkl. Nachlass (netto)		
Umsatzsteuer		
Summe (brutto)		

Verfahren: 20261019 - Netzbetrieb Managed Service

AUFLISTUNG ALLER DATEIANLAGEN ZU DEN POSITIONEN

Name	Dateiname	Größe	MIME-Type
------	-----------	-------	-----------

EIGNUNGSKRITERIEN

1 Wichtige Hinweise zu den Eignungskriterien [Mussangabe]

Der Auftraggeber hat öffentliche Aufträge an fachkundige und leistungsfähige (geeignete) Unternehmen zu vergeben (§ 122 GWB und § 31 UVgO).

Ein Unternehmen (Bewerber/Bieter/Unterauftragnehmer) ist geeignet, wenn die im Nachfolgenden festgelegten Kriterien im Hinblick auf die Befähigung und Erlaubnis der Berufsausübung, wirtschaftliche und finanzielle Leistungsfähigkeit sowie technische und berufliche Leistungsfähigkeit erfüllt bzw. beantwortet sind.

Als vorläufigen Beleg der Eignung eines Unternehmens hat der Auftraggeber grundsätzlich die Vorlage von Eigenerklärungen zu akzeptieren (§ 48 Abs. 2 VgV und § 35 Abs. 2 UVgO). Die Eigenerklärungen werden durch Beantwortung des Kriterienkatalogs abgegeben. Dabei ist folgendes zu beachten:

- Ausschlusskriterien (K.O.-Kriterium: Ja) müssen erfüllt werden. Angebote, die ein oder mehrere Ausschlusskriterien nicht erfüllen (Fragen mit "Nein" beantwortet), werden ausgeschlossen.

- Pflichtangaben (Mussangabe) sind zwingend erforderliche Angaben. Fragen können auch mit "Nein" beantwortet werden, ohne dass dies zwingend zum Ausschluss des Angebotes führt. Angebote deren Angaben jedoch nicht erkennen lassen, dass das Unternehmen über die erforderliche Eignung für die ordnungsgemäße Ausführung des Auftrags verfügt, können gleichwohl ausgeschlossen werden.

- Falls mit Angebotsabgabe vom Unternehmen gesonderte Nachweise vorzulegen sind, wird darauf im Kriterium/in der Frage hingewiesen.

Der Auftraggeber behält sich das Recht vor, noch im Vergabeverfahren (vor Zuschlagserteilung) und auch während der Vertragslaufzeit aktuelle Nachweise, Bestätigungen und Bescheinigungen für die vom Unternehmen bzw. Auftragnehmer mit seinem Angebot abgegebenen Erklärungen unter einer Fristsetzung einzufordern. Eine wissentliche falsche Angabe der Erklärungen kann den Ausschluss von diesem und weiterer Vergabeverfahren zur Folge haben.

☐ Ich erkläre/Wir erklären, dass ich/wir die vorgenannten Hinweise zu den Eignungskriterien zur Kenntnis genommen haben.

Mehrere Antworten wählbar

2 Hinweis zum Wettbewerbsregister

Ab einer Auftragssumme von 30.000 Euro wird der Auftraggeber von den Bewerbern, welche zur Angebotsabgabe aufgefordert werden sollen bzw. von dem Bieter, auf dessen Angebot der Zuschlag erteilt werden soll, einen Auszug aus dem Wettbewerbsregister gem. Wettbewerbsregistergesetz beim Bundeskartellamt anfordern.

3 Erklärungen zum Unternehmensprofil

Gewichtung: 0,00%

3.1 Bewerber-/Bieterstruktur [Mussangabe]

Ich/Wir beabsichtige/n am Vergabeverfahren als Einzelbewerber/-bieter teilzunehmen:

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

3.2 Bieter-/Arbeitsgemeinschaft [Mussangabe]

Ich/Wir beabsichtige/n als Bieter-/Arbeitsgemeinschaft am Vergabeverfahren teilzunehmen:
(Falls Ja, ist das Formblatt "Anlage EBG - Eigenerklärung zur Bietergemeinschaft" ausgefüllt mit dem Angebot einzureichen)

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

3.3 Unterauftragnehmer/Nachunternehmer [Mussangabe]

Ich/Wir beabsichtige/n zur Erfüllung des Auftrags Unterauftragnehmer bzw. Nachunternehmer einzusetzen:
(Falls Ja, ist das Formblatt "Anlage EN1-Eigenerklärung Nachunternehmereinsatz" und das Formblatt "Anlage EN2-Verpflichtungserklärung Nachunternehmer" mit dem Angebot einzureichen)

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

3.4 Eintragung im Berufs-/Handelsregister [Mussangabe]

Ich/Wir bin/sind im Berufs-/Handelsregister eingetragen:

(Hinweis: Auf Verlangen der Vergabestelle ist ein aktueller Handelsregisterauszug -nicht älter als sechs Monate- vom Unternehmen vorzulegen)

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

3.5 Angaben zum Berufs-/Handelsregistereintrag [Mussangabe]

Falls Ihr Unternehmen im öffentlichen Berufs-/Handelsregister eingetragen ist, sind die folgenden Angaben in der vorgegebenen Reihenfolge zu tätigen:

- Rechtsform des Unternehmens
- Registernummer
- Amtsgericht
- Sitz des Unternehmens (Straße Nr., PLZ, Ort)
- USt.ID-Nr.

3.6 informative Abfrage [Mussangabe]

Bitte geben Sie, in dieser Reihenfolge, an:

- Name der Ansprechperson im Unternehmen mit e-Mail Adresse und Telefonnummer
- E-Mail Adresse für Bestellaufträge
- Bank-Name
- IBAN
- ggf. SWIFT

3.7 KMU-Eigenschaft [Mussangabe]

Angabe für statistische Zwecke (VergStatVO)

Ich/Wir bin/sind ein kleines oder mittleres Unternehmen (KMU):

Hinweis: Ihr Unternehmen erfüllt die KMU-Eigenschaft, wenn weniger als 250 Personen beschäftigt sind und ein Jahresumsatz von höchstens 50 Mio. EUR oder eine Jahresbilanzsumme von höchstens 43 Mio. EUR erzielt wird.

- ☐ Keine Angabe (0)
☐ Kleinstunternehmen (0)
☐ Kleines Unternehmen (0)
☐ Mittleres Unternehmen (0)
☐ Großes Unternehmen (kein KMU) (0)

Nur eine Antwort wählbar

4 Erklärungen zur Zuverlässigkeit, Fachkunde und Leistungsfähigkeit

Gewichtung: 0,00%

4.1 Umsatz [Mussangabe]

Ausschlusskriterium

Ich/Wir erkläre/n, dass mein/unser Unternehmen in den letzten drei Geschäftsjahren einen Gesamtumsatz von mehr als XXX.XXX EUR netto pro Jahr (entspricht max. das Zweifache des geschätzten Auftragswertes gem. § 45 Abs. 2 VgV) erzielt hat.

- ☐ Keine Angabe
☐ Ja
☐ Nein

Nur eine Antwort wählbar

4.2 Umsätze [Mussangabe]

Bitte geben Sie die Umsätze Ihres Unternehmens in den letzten drei abgeschlossenen Geschäftsjahren an.

4.3 Berufsgenossenschaft [Mussangabe]

Ich/Wir bin/sind Mitglied der Berufsgenossenschaft:

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.4 Insolvenz und Liquidation [Mussangabe]

Ich/Wir erkläre/n, dass ein Insolvenzverfahren oder ein vergleichbares gesetzlich geregeltes Verfahren weder beantragt noch eröffnet wurde, ein Antrag auf Eröffnung nicht mangels Masse abgelehnt wurde und sich mein/unser Unternehmen nicht in Liquidation befindet.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

4.5 Strafrechtliche Ermittlungen [Mussangabe]

Ich/Wir erkläre/n, dass keine aktuellen strafrechtlichen Ermittlungen gegen Mitglieder der Geschäftsleitung/Objekte itung anhängig sind.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.6 Steuern, Abgaben und Sozialbeiträge [Mussangabe]

Ich/Wir erkläre/n, dass ich/wir meine/unsere Verpflichtung zur Zahlung von Steuern und Abgaben sowie der Beiträge zur gesetzlichen Sozialversicherung, soweit sie der Pflicht zur Beitragszahlung unterfallen, ordnungsgemäß erfüllt habe/n.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.7 Betriebs-/Berufshaftpflichtversicherung [Mussangabe]

Ich/Wir erkläre/n, dass ich/wir über eine Betriebs-/Berufshaftpflichtversicherung verfüge/n, die mindestens die nachstehenden Schäden mit folgenden Deckungssummen abdeckt:

- Für Personen-, Sach- und Vermögensschäden mindestens 2.500.000 EUR pauschal je Schadensfall einfach maximiert pro Jahr und ich/wir diese während der gesamten Vertragslaufzeit aufrechterhalten werde/n
- oder
- im Auftragsfalle eine entsprechende Versicherung abschließen werde/n bzw. eine entsprechende Anpassung der Versicherungsdeckungssumme vornehmen werde/n und ich/wir diese während der gesamten Vertragslaufzeit aufrechterhalten werde/n.

- ☐ Keine Angabe (0)
☐ Ja (0)
☐ Nein (0)

Nur eine Antwort wählbar

4.8 Nichtvorliegen von Ausschlussgründen (§ 123 GWB) [Mussangabe]

Ausschlusskriterium

Ich/Wir erkläre/n, dass keine der nach § 123 GWB genannten und nachfolgende abgedruckten Ausschlussgründe vorliegen:

Nach § 123 Abs. 1 GWB ist ein Unternehmen von der Teilnahme an einem Vergabeverfahren wegen Unzuverlässigkeit auszuschließen, wenn der Auftraggeber Kenntnis davon hat, dass eine Person, deren Verhalten dem Unternehmen zuzurechnen ist, rechtskräftig verurteilt ist wegen:

1. § 129 des Strafgesetzbuchs (Bildung krimineller Vereinigungen), § 129a des Strafgesetzbuchs (Bildung terroristischer Vereinigungen) oder § 129b des Strafgesetzbuchs (Kriminelle und terroristische Vereinigungen im Ausland),
2. § 89c des Strafgesetzbuchs (Terrorismusfinanzierung) oder wegen der Teilnahme an einer solchen Tat oder wegen der Bereitstellung oder Sammlung finanzieller Mittel in Kenntnis dessen, dass diese finanziellen Mittel ganz oder teilweise dazu verwendet werden oder verwendet werden sollen, eine Tat nach § 89a Absatz 2 Nummer 2 des Strafgesetzbuchs zu begehen,
3. § 261 des Strafgesetzbuchs (Geldwäsche),
4. § 263 des Strafgesetzbuchs (Betrug), soweit sich die Straftat gegen den Haushalt der Europäischen Union oder gegen Haushalte richtet, die von der Europäischen Union oder in ihrem Auftrag verwaltet werden,
5. § 264 des Strafgesetzbuchs (Subventionsbetrug), soweit sich die Straftat gegen den Haushalt der Europäischen Union oder gegen Haushalte richtet, die von der Europäischen Union oder in ihrem Auftrag verwaltet werden,
6. § 299 des Strafgesetzbuchs (Bestechlichkeit und Bestechung im geschäftlichen Verkehr), §§ 299a und 299b des Strafgesetzbuchs (Bestechlichkeit und Bestechung im Gesundheitswesen),
7. § 108e des Strafgesetzbuchs (Bestechlichkeit und Bestechung von Mandatsträgern) oder § 108f des Strafgesetzbuchs (unzulässige Interessenwahrnehmung),
8. den §§ 333 und 334 des Strafgesetzbuchs (Vorteilsgewährung und Bestechung), jeweils auch in Verbindung mit § 335a des Strafgesetzbuchs (Ausländische und internationale Bedienstete),
9. Artikel 2 § 2 des Gesetzes zur Bekämpfung internationaler Bestechung (Bestechung ausländischer Abgeordneter im Zusammenhang mit internationalem Geschäftsverkehr) oder
10. den §§ 232, 232a Absatz 1 bis 5, den §§ 232b bis 233a des Strafgesetzbuchs (Menschenhandel, Zwangsprostitution, Zwangsarbeit, Ausbeutung der Arbeitskraft, Ausbeutung unter Ausnutzung einer Freiheitsberaubung).

Einem Verstoß gegen diese Vorschriften gleichgesetzt sind Verstöße gegen entsprechende Strafnormen anderer Staaten. Ein Verhalten einer rechtskräftig verurteilten Person ist einem Unternehmen zuzurechnen, wenn sie für dieses Unternehmen bei der Führung der Geschäfte selbst verantwortlich gehandelt hat oder ein Aufsichts- oder Organisationsverschulden gemäß § 130 des Gesetzes über Ordnungswidrigkeiten (OWiG) einer Person im Hinblick auf das Verhalten einer anderen für das Unternehmen handelnden, rechtskräftig verurteilten Person vorliegt.

- ☐ Keine Angabe
☐ Ja
☐ Nein

Nur eine Antwort wählbar

4.9 Nichtvorliegen von Ausschlussgründen (§ 124 GWB) [Mussangabe]

Ich/Wir erkläre/n, dass keine der nach § 124 GWB genannten und nachfolgende abgedruckten Ausschlussgründe vorliegen:

Nach § 124 GWB können öffentliche Auftraggeber unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit ein Unternehmen zu jedem Zeitpunkt des Vergabeverfahrens von der Teilnahme an einem Vergabeverfahren ausschließen, wenn

1. das Unternehmen bei der Ausführung öffentlicher Aufträge nachweislich gegen geltende umwelt-, sozial- oder arbeitsrechtliche Verpflichtungen verstoßen hat,
2. das Unternehmen zahlungsunfähig ist, über das Vermögen des Unternehmens ein Insolvenzverfahren oder ein vergleichbares Verfahren beantragt oder eröffnet worden ist, die Eröffnung eines solchen Verfahrens mangels Masse abgelehnt worden ist, sich das Unternehmen im Verfahren der Liquidation befindet oder seine Tätigkeit eingestellt hat,
3. das Unternehmen im Rahmen der beruflichen Tätigkeit nachweislich eine schwere Verfehlung begangen hat, durch die die Integrität des Unternehmens infrage gestellt wird; § 123 Absatz 3 ist entsprechend anzuwenden,
4. der öffentliche Auftraggeber über hinreichende Anhaltspunkte dafür verfügt, dass das Unternehmen Vereinbarungen mit anderen Unternehmen getroffen hat, die eine Verhinderung, Einschränkung oder Verfälschung des Wettbewerbs bezwecken oder bewirken,
5. ein Interessenkonflikt bei der Durchführung des Vergabeverfahrens besteht, der die Unparteilichkeit und Unabhängigkeit einer für den öffentlichen Auftraggeber tätigen Person bei der Durchführung des Vergabeverfahrens beeinträchtigen könnte und der durch andere, weniger einschneidende Maßnahmen nicht wirksam beseitigt werden kann,
6. eine Wettbewerbsverzerrung daraus resultiert, dass das Unternehmen bereits in die Vorbereitung des Vergabeverfahrens einbezogen war, und diese Wettbewerbsverzerrung nicht durch andere, weniger einschneidende Maßnahmen beseitigt werden kann,
7. das Unternehmen eine wesentliche Anforderung bei der Ausführung eines früheren öffentlichen Auftrags oder Konzessionsvertrags erheblich oder fortdauernd mangelhaft erfüllt hat und dies zu einer vorzeitigen Beendigung, zu Schadensersatz oder zu einer vergleichbaren Rechtsfolge geführt hat,
8. das Unternehmen in Bezug auf Ausschlussgründe oder Eignungskriterien eine schwerwiegende Täuschung begangen oder Auskünfte zurückgehalten hat oder nicht in der Lage ist, die erforderlichen Nachweise zu übermitteln, oder
9. das Unternehmen
 - a) versucht hat, die Entscheidungsfindung des öffentlichen Auftraggebers in unzulässiger Weise zu beeinflussen,
 - b) versucht hat, vertrauliche Informationen zu erhalten, durch die es unzulässige Vorteile beim Vergabeverfahren erlangen könnte, oder
 - c) fahrlässig oder vorsätzlich irreführende Informationen übermittelt hat, die die Vergabeentscheidung des öffentlichen Auftraggebers erheblich beeinflussen könnten, oder versucht hat, solche Informationen zu übermitteln.

- ☐] Keine Angabe (0)
☐] Ja (0)
☐] Nein (0)

Nur eine Antwort wählbar

4.10 Lieferkettensorgfaltspflichten gesetz [Mussangabe]

Wir erklären, dass uns keine Verstöße gegen menschrechtliche (gem. § 2 Abs. 2 Nr. 1-12 LkSG) und umweltbezogene Pflichten (gem. § 2 Abs. 3 Nr. 1-8 LkSG) innerhalb unseres Unternehmens und der Unternehmen unserer Zulieferer bekannt sind. Sollten wir Kenntnis darüber erlangen, dass in unserem Unternehmen oder in einem Unternehmen unserer Zulieferer eine Verletzung menschenrechtlicher oder umweltbezogener Pflichten stattfindet/stattgefunden hat, so werden wir das UKF hierüber unverzüglich informieren.

- ☐] Keine Angabe (0)
☐] Ja (0)
☐] Nein (0)

Nur eine Antwort wählbar

4.11 Referenzen

Gewichtung: 0,00%

4.11.1 Referenzen

Referenzen müssen abgeschlossene oder seit mindestens 12 Monaten laufende Leistungen betreffen. Die Leistungen müssen in Art und Umfang mit dem ausgeschriebenen Managed Service vergleichbar sein.

4.11.2 Erklärung Referenzen 1 [Mussangabe]

Ausschlusskriterium

Der Bieter weist mindestens eine Referenz über den laufenden Betrieb einer LAN-/WLAN-Umgebung mit zentralem Betriebsmodell, Monitoring, Incident-, Problem-, Change- und Reporting-Prozessen nach. Die Referenz muss mindestens 500 aktive Netzwerkkomponenten oder eine vergleichbar komplexe, verteilte Infrastruktur umfassen.

- ☐] Keine Angabe
☐] Ja
☐] Nein

Nur eine Antwort wählbar

4.11.3 Referenzen 1

Nachfolgend sind die Referenzen genau zu benennen. Jede einzelne Referenz muss den genannten Mindestanforderungen genügen.

4.11.4 Referenzeingabe Nr. 1 [Mussangabe]

Es müssen folgende Angaben in der vorgegebenen Reihenfolge getätigt werden:

- Benennung Referenzauftraggeber (mit Name und Anschrift)
- Benennung Ansprechpartner (mit Name, Telefonnummer und E-Mail)
- Bezeichnung des Auftragsgegenstandes
- Beschreibung des Leistungsumfanges
- Auftragsvolumen (in EUR netto)
- Ausführungszeitraum (von Datum bis Datum)

Ich/Wir erkläre/n mich/uns durch die Angabe der Referenz mit einer Nachfrage des Auftraggebers beim jeweiligen Referenzauftraggeber einverstanden. Die Einreichung einer Bescheinigung der Referenzauftraggeber ist daher nicht erforderlich.

4.11.5 Erklärung Referenzen 2 [Mussangabe]

Ausschlusskriterium

Betrieb Cisco-basierter Enterprise-Netzwerke

Der Bieter weist mindestens eine Referenz über den Betrieb einer Cisco-basierten Enterprise-Netzwerkinfrastuktur nach. Die Referenz muss Switching, Routing, WLAN-Betrieb oder zentrale Cisco-Management-/Controlerkomponenten umfassen.

- ☐ Keine Angabe
☐ Ja
☐ Nein

Nur eine Antwort wählbar

4.11.6 Referenzen 2

Nachfolgend sind die Referenzen genau zu benennen. Jede einzelne Referenz muss den genannten Mindestanforderungen genügen.

4.11.7 Referenzeingabe Nr. 2 [Mussangabe]

Es müssen folgende Angaben in der vorgegebenen Reihenfolge getätigt werden:

- Benennung Referenzauftraggeber (mit Name und Anschrift)
- Benennung Ansprechpartner (mit Name, Telefonnummer und E-Mail)
- Bezeichnung des Auftragsgegenstandes
- Beschreibung des Leistungsumfanges
- Auftragsvolumen (in EUR netto)
- Ausführungszeitraum (von Datum bis Datum)

Ich/Wir erkläre/n mich/uns durch die Angabe der Referenz mit einer Nachfrage des Auftraggebers beim jeweiligen Referenzauftraggeber einverstanden. Die Einreichung einer Bescheinigung der Referenzauftraggeber ist daher nicht erforderlich.

4.12 Fachkräfte und Qualität

Gewichtung: 0,00%

4.12.1 Business Continuity / Notbetrieb [Mussangabe]

Ausschlusskriterium

Der Bieter bestätigt, dass er für die angebotenen Managed-Service-Leistungen angemessene Regelungen zur Business Continuity, zum Notbetrieb und zur Wiederherstellung kritischer Servicefunktionen vorhält. Dies umfasst insbesondere Ausfälle eigener Betriebsplattformen, Personal- oder Kommunikationsausfälle sowie Sicherheitsvorfälle beim Bewerber selbst.

- ☐ Keine Angabe
☐ Ja
☐ Nein

Nur eine Antwort wählbar

4.12.2 ISO 27001 [Mussangabe]

Ausschlusskriterium

ISO 27001 - Informationssicherheits-Managementsystem Der Bewerber verfügt über eine gültige Zertifizierung nach ISO/IEC 27001 in der aktuellen Normfassung. Der Nachweis kann mittels Eignungsleihe erbracht werden, sofern der eignungsleihende Nachunternehmer an der Leistungserbringung beteiligt ist.

Bitte gültiges Zertifikat vorlegen.

- ☐ Keine Angabe
☐ Ja
☐ Nein

Nur eine Antwort wählbar

4.12.3 ISO 9001 [Mussangabe]

Ausschlusskriterium

ISO 9001 - Qualitätsmanagementsystem Der Bewerber verfügt über eine gültige Zertifizierung nach ISO 9001 in der aktuellen Normfassung. Der Nachweis kann mittels Eignungsleihe erbracht werden, sofern der eignungsleihende Nachunternehmer an der Leistungserbringung beteiligt ist.

Bitte gültiges Zertifikat vorlegen.

- ☐ Keine Angabe
☐ Ja
☐ Nein

Nur eine Antwort wählbar

4.12.4 DSGVO [Mussangabe]

Ausschlusskriterium

DSGVO-Konformität und Vertraulichkeit Der Bewerber stellt sicher, dass alle im Rahmen des Managed Service verarbeiteten Betriebs-, Monitoring-, Ticket-, Konfigurations- und Assetdaten DSGVO-konform, vertraulich und nach den Sicherheitsvorgaben des Auftraggebers verarbeitet werden.

Durch ankreuzten von "JA" bestätigen Sie die Erfüllung dieses Kriteriums. Alle anderen Angaben führen zum Ausschluss.

- ☐ ☐ Keine Angabe
☐ ☐ Ja
☐ ☐ Nein

Nur eine Antwort wählbar

4.12.5 EU/EWR-Datenverarbeitung [Mussangabe]

Ausschlusskriterium

EU/EWR-Datenverarbeitung Betriebs-, Monitoring-, Ticket-, Konfigurations- und Assetdaten des Auftraggebers werden ausschließlich innerhalb der EU bzw. des EWR verarbeitet und gespeichert, sofern der Auftraggeber nicht im Einzelfall ausdrücklich etwas anderes freigibt. Subunternehmer und Verarbeitungsorte sind offenzulegen.

Durch ankreuzten von "JA" bestätigen Sie die Erfüllung dieses Kriteriums. Alle anderen Angaben führen zum Ausschluss. Für Subunternehmer ist bitte eine gesonderte Eigenerklärung beizulegen.

- ☐ ☐ Keine Angabe
☐ ☐ Ja
☐ ☐ Nein

Nur eine Antwort wählbar

4.12.6 Deutschsprachige Servicekoordination [Mussangabe]

Ausschlusskriterium

Deutschsprachige Servicekoordination Kommunikation mit dem Auftraggeber, Service Delivery Management, Eskalation, Betriebsberichte, Regelmeetings und Dokumentation sind in deutscher Sprache zu erbringen. Hersteller Eskalationen können in englischer Sprache erfolgen, sofern die Kommunikation gegenüber dem Auftraggeber deutschsprachig bleibt.

Durch ankreuzten von "JA" bestätigen Sie die Erfüllung dieses Kriteriums. Alle anderen Angaben führen zum Ausschluss.

- ☐ ☐ Keine Angabe
☐ ☐ Ja
☐ ☐ Nein

Nur eine Antwort wählbar

4.12.7 Cisco-Bestandsbetrieb im EnterpriseLAN/WLAN-Umfeld [Mussangabe]

Ausschlusskriterium

Cisco-Bestandsbetrieb im Enterprise-LAN-/WLAN-Umfeld Der Bewerber weist nach, dass er den Betrieb einer Cisco-basierten Enterprise-LAN-/WLAN-Infrastruktur fachlich, organisatorisch und personell beherrscht. Der Nachweis umfasst Switching, Routing, WLAN-Controller, Access Points, Managementsysteme, Konfigurationssicherung, Troubleshooting, Release-/Firmwarebewertung und Herstellerfallbearbeitung.

Durch ankreuzten von "JA" bestätigen Sie die Erfüllung dieses Kriteriums. Alle anderen Angaben führen zum Ausschluss. Bitte fügen Sie eine Eigenerklärung mit Darstellung der Rollen, Qualifikationen, Zertifizierungen und praktischen Betriebserfahrung bei.

- ☐ ☐ Keine Angabe
☐ ☐ Ja
☐ ☐ Nein

Nur eine Antwort wählbar

4.12.8 Personalnachweis CCNP Enterprise (Mindestanzahl) [Mussangabe]

Ausschlusskriterium

Personalnachweis CCNP Enterprise (Mindestanzahl 5 MA) Der Bewerber weist nach, dass er mindestens fünf (5) Mitarbeiter im eingesetzten Betriebsteam beschäftigt, die über eine gültige Cisco-Zertifizierung CCNP Enterprise verfügen.

Durch ankreuzten von "JA" bestätigen Sie die Erfüllung dieses Kriteriums. Alle anderen Angaben führen zum Ausschluss.

Bitte fügen Sie eine Eigenerklärung mit Angabe der Anzahl CCNP-zertifizierter Mitarbeiter bei. Zertifikate sind einzureichen.

- ☐ ☐ Keine Angabe
☐ ☐ Ja
☐ ☐ Nein

Nur eine Antwort wählbar

4.12.9 Personalnachweis CCIE Enterprise Infrastructure [Mussangabe]

Ausschlusskriterium

Personalsnachweis CCIE Enterprise Infrastructure (Mindestanzahl Anzahl + Name Technical Lead, min. 2) Der Bewerber weist nach, dass er mindestens zwei (2) Mitarbeiter im eingesetzten Betriebsteam beschäftigt, die über eine gültige Cisco-Zertifizierung CCIE Enterprise Infrastructure verfügen. Mindestens einer ist als Technical Lead namentlich zu benennen.

Durch ankreuzten von "JA" bestätigen Sie die Erfüllung dieses Kriteriums. Alle anderen Angaben führen zum Ausschluss. Beizufügen sind: Eigenerklärung mit Angabe der Anzahl CCIE-zertifizierter Mitarbeiter sowie Name des Technical Lead; Nachweis: Zertifikat

- ☐] Keine Angabe
☐] Ja
☐] Nein

Nur eine Antwort wählbar

5 Verpflichtungserklärung Tariftreue und Mindestlohn [Mussangabe]

Verpflichtungserklärung zu Tariftreue und Mindestentgelt bei öffentlichen Aufträgen nach dem Hessischen Vergabe- und Tariftreuegesetz (HVTG) vom 19. Dezember 2014, GVBl. S. 354

Es wird darauf hingewiesen, dass sich die Verpflichtungserklärung zu Tariftreue und Mindestentgelt entsprechend den Vorgaben der §§ 4 und 6 des Hessischen Vergabe- und Tariftreuegesetzes (HVTG) zur Zahlung des Mindestlohns gemäß § 20 des Mindestlohngesetzes (MiLoG) bzw. des Tariflohns nach dem Arbeitnehmer-Entsendegesetz (AEntG) nicht auf Beschäftigte bezieht, die bei einem Bieter oder Nachunternehmer im EU-Ausland beschäftigt sind und die Leistung im EU-Ausland erbringen.

Ich/Wir erkläre/n:

1. Ich/wir nehme/n zur Kenntnis, dass ich/wir gemäß § 4 Abs. 1 HVTG die für mich/uns geltenden gesetzlichen, aufgrund eines Gesetzes festgesetzten und unmittelbar geltenden tarifvertraglichen Leistungen zu gewähren habe/n. Ich/wir nehme/n weiterhin zur Kenntnis, dass bei Vorliegen von Anhaltspunkten dafür, dass gegen diese Regelung verstoßen wird, auf Anforderung dem öffentlichen Auftraggeber oder dem Besteller die Einhaltung dieser Verpflichtung nachzuweisen ist.
2. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 2 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung diejenigen Arbeitsbedingungen einschließlich des Entgelts zu gewähren, die nach Art und Höhe mindestens den Vorgaben desjenigen Tarifvertrags entsprechen, an den mein/unser Unternehmen aufgrund des AEntG gebunden ist.
3. Ich/wir verpflichte/n mich/uns, gemäß § 4 Abs. 3 und § 6 HVTG meinen/unseren Beschäftigten bei der Ausführung der Leistung ein Entgelt zu zahlen, das den Vorgaben des MiLoG entspricht. Im Falle der Auftragsausführung durch Nachunternehmer oder Verleihunternehmen sind im Angebot, soweit diese bereits bei Angebotsabgabe bekannt sind, spätestens jedoch vor Beginn der Ausführung der Leistung durch das Nachunternehmen oder Verleihunternehmen die entsprechenden Erklärungen in Textform abzugeben und vorzulegen.
 - Die Erklärung kann entfallen, soweit sie bereits in einem Präqualifizierungsregister hinterlegt ist.
 - Die Einhaltung der nach Bundesrecht oder aufgrund von Bundesrecht für mich/uns geltenden Regelungen von besonders festgesetzten Mindestentgelten (Mindestlohn) als Mindeststandard im Angebot entfällt, soweit nach § 4 HVTG Tariftreue gefordert werden kann und die danach maßgebliche tarifliche Regelung für die Beschäftigten günstiger ist als die für sie nach Bundesrecht geltenden Bestimmungen.
4. Ich/wir erkläre/n, dass ich/wir nicht wegen eines Verstoßes gegen § 21 MiLoG (Bußgeldvorschriften) mit einer Geldbuße von wenigstens 2.500 Euro belegt worden bin/sind und damit nicht die Voraussetzungen für einen Ausschluss von der Auftragsvergabe nach § 19 Abs. 1 und 3 MiLoG vorliegen.
5. Ich/wir verpflichte/n mich/uns für den Fall der Ausführung vertraglich übernommener Leistungen durch Nachunternehmen, die Erfüllung der Verpflichtungen nach den §§ 4 und 6 HVTG durch die Nachunternehmen sicherzustellen und dem öffentlichen Auftraggeber Tariftreue- und sonstige Verpflichtungs- sowie Mindestlohnserklärungen der Nachunternehmen nach Auftragserteilung, spätestens vor Beginn der Ausführung der Leistung durch das Nachunternehmen, vorzulegen. Gleiches gilt, wenn ich/wir oder ein beauftragtes Nachunternehmen zur Ausführung des Auftrags Arbeitskräfte eines Verleihunternehmens einsetze(n)/einsetzt. Diese Verpflichtung gilt entsprechend auch für alle weiteren Nachunternehmen und Verleihunternehmen.

☐] Ich/ Wir bestätige/n, dass vorstehende Angaben von meinem/ unserem Unternehmen bei der Angebotenen Leistung erfüllt sind.

Mehrere Antworten wählbar

6 Eigenerklärung bzgl. Sanktionen gegen Russland [Mussangabe]

Die nachfolgende Erklärung gebe/n ich/wir verbindlich ab (ggf. zugleich in Vertretung für die lt. Teilnahmeantrag / Angebot Vertretenen auch für diese):

1. Der / die Bewerber / Bieter gehört / gehören nicht zu den in Artikel 5 k) Absatz 1 der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 über restriktive Maßnahmen angesichts der Handlungen Russlands, die die Lage in der Ukraine destabilisieren, genannten Personen oder Unternehmen, die einen Bezug zu Russland im Sinne der Vorschrift aufweisen,
 - a) durch die russische Staatsangehörigkeit des Bewerbers/Bieters oder die Niederlassung des Bewerbers/Bieters in Russland,
 - b) durch die Beteiligung einer natürlichen Person oder eines Unternehmens, auf die eines der Kriterien nach Buchstabe a zutrifft, am Bewerber/Bieter über das Halten von Anteilen im Umfang von mehr als 50%,
 - c) durch das Handeln der Bewerber/Bieter im Namen oder auf Anweisung von Personen oder Unternehmen, auf die die Kriterien der Buchstaben a und/oder b zutrifft.
2. Die am Auftrag als Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden, beteiligten Unternehmen, auf die mehr als 10 % des Auftragswerts entfällt, gehören ebenfalls nicht zu dem in der Vorschrift genannten Personenkreis mit einem Bezug zu Russland im Sinne der Vorschrift.
3. Es wird bestätigt und sichergestellt, dass auch während der Vertragslaufzeit keine als Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Zusammenhang mit der Erbringung des Eignungsnachweises in Anspruch genommen werden, beteiligten Unternehmen eingesetzt werden, auf die mehr als 10 % des Auftragswerts entfällt.

7 Artikel 5k der Verordnung (EU) Nr. 833/2014

Artikel 5k der Verordnung (EU) Nr. 833/2014 in der Fassung des Art. 1 Ziff. 23 der Verordnung (EU) 2022/576 des Rates vom 8. April 2022 lautet wie folgt:

- (1) Es ist verboten, öffentliche Aufträge oder Konzessionen, die in den Anwendungsbereich der Richtlinien über die öffentliche Auftragsvergabe sowie unter Artikel 10 Absatz 1, Absatz 3, Absatz 6 Buchstaben a bis e, Absatz 8, Absatz 9 und Absatz 10 und die Artikel 11, 12, 13 und 14 der Richtlinie 2014/23/EU, unter die Artikel 7 und 8, Artikel 10 Buchstaben b bis f und h bis j der Richtlinie 2014/24/EU, unter Artikel 18, Artikel 21 Buchstaben b bis e und g bis i, Artikel 29 und Artikel 30 der Richtlinie 2014/25/EU und unter Artikel 13 Buchstaben a bis d, f bis h und j der Richtlinie 2009/81/EG fallen, an folgende Personen, Organisationen oder Einrichtungen zu vergeben bzw. Verträge mit solchen Personen, Organisationen oder Einrichtungen weiterhin zu erfüllen:
- a) russische Staatsangehörige oder in Russland niedergelassene natürliche oder juristische Personen, Organisationen oder Einrichtungen,
 - b) juristische Personen, Organisationen oder Einrichtungen, deren Anteile zu über 50 % unmittelbar oder mittelbar von einer der unter Buchstabe a genannten Organisationen gehalten werden, oder
 - c) natürliche oder juristische Personen, Organisationen oder Einrichtungen, die im Namen oder auf Anweisung einer der unter Buchstabe a oder b genannten Organisationen handeln, auch solche, auf die mehr als 10 % des Auftragswerts entfällt, Unterauftragnehmer, Lieferanten oder Unternehmen, deren Kapazitäten im Sinne der Richtlinien über die öffentliche Auftragsvergabe in Anspruch genommen werden.
- (2) Abweichend von Absatz 1 können die zuständigen Behörden die Vergabe oder die Fortsetzung der Erfüllung von Verträgen genehmigen, die bestimmt sind für
- a) den Betrieb ziviler nuklearer Kapazitäten, ihre Instandhaltung, ihre Stilllegung, die Entsorgung ihrer radioaktiven Abfälle, ihre Versorgung mit und die Wiederaufbereitung von Brennelementen und die Weiterführung der Planung, des Baus und die Abnahmetests für die Indienststellung ziviler Atomanlagen und ihre Sicherheit sowie die Lieferung von Ausgangsstoffen zur Herstellung medizinischer Radioisotope und ähnlicher medizinischer Anwendungen, kritischer Technologien zur radiologischen Umweltüberwachung sowie für die zivile nukleare Zusammenarbeit, insbesondere im Bereich Forschung und Entwicklung,
 - b) die zwischenstaatliche Zusammenarbeit bei Raumfahrtprogrammen,
 - c) die Bereitstellung unbedingt notwendiger Güter oder Dienstleistungen, wenn sie ausschließlich oder nur in ausreichender Menge von den in Absatz 1 genannten Personen bereitgestellt werden können,
 - d) die Tätigkeit der diplomatischen und konsularischen Vertretungen der Union und der Mitgliedstaaten in Russland, einschließlich Delegationen, Botschaften und Missionen, oder internationaler Organisationen in Russland, die nach dem Völkerrecht Immunität genießen.
 - e) den Kauf, die Einfuhr oder die Beförderung von Erdgas und Erdöl, einschließlich raffinierter Erdölzeugnisse, sowie von Titan, Aluminium, Kupfer, Nickel, Palladium und Eisenerz aus oder durch Russland in die Union, oder
 - f) den Kauf, die Einfuhr oder die Beförderung von Kohle und anderen festen fossilen Brennstoffen, die in Anhang XXII aufgeführt sind, bis 10. August 2022.
- (3) Der betreffende Mitgliedstaat unterrichtet die anderen Mitgliedstaaten und die Kommission über jede nach diesem Artikel erteilte Genehmigung innerhalb von zwei Wochen nach deren Erteilung.
- (4) Die Verbote gemäß Absatz 1 gelten nicht für die Erfüllung — bis zum 10. Oktober 2022 — von Verträgen, die vor dem 9. April 2022 geschlossen wurden.

Verfahren: 20261019 - Netzbetrieb Managed Service

LEISTUNGSKRITERIEN

1 Wird durch den Auftraggeber ausgefüllt.

Gewichtung: 100,00%
Maximalpunktzahl: 60

Entspricht der Punktzahl der Anlage Z Zuschlagskriterien und Anlage A Anforderungen an die Lösungsansätze

Typ	Dateiname	Größe	MIME-Type
Dateianlage	Anlage P - Preismatrix Version 3 Korrektur 14.07.2026.xlsx	36,16 KB	xlsx
Dateianlage	Anlage CR-Verfahren Stand 16.07.2026.pdf	239,30 KB	pdf