

EVB-IT-Dienstleistungsvertrag

Leistungsbeschreibung – Managed Service „C3000 Faxserver“

Version: 1.4

Datum: 22.05.2026

1. Ziel und Gegenstand der Leistung

Gegenstand der Ausschreibung ist der Abschluss eines EVB-IT-Dienstleistungsvertrags für Implementierung, Betrieb, Wartung und technische Betreuung eines dedizierten, hochverfügbaren Faxdienstes auf Basis Avaya C3000 (Stand-Alone) inklusive 3rd-Level-Support beim Hersteller.

Optional können Voice-Sprachboxen bzw. Anrufbeantworter beauftragt werden.

Nicht Gegenstand sind SIP-Trunk, SBC, Office-Telefonie, Unified Communications, Contact Center und Endgeräte.

Der C3000-Faxdienst ist in Betrieb und wird aktuell durch die Firma Avaya als Managed Service erbracht. Aufgrund des Vertragsendes erfolgt eine Neuausschreibung des Betriebs und der Schwenk auf die neue SBC-Umgebung. Ziel ist, den C3000 in einer Systemumgebung, bestehend aus Microsoft Teams und einem Omnichannel Contact Center, der sogenannten Omnikanalplattform (OKP), stabil zu betreiben.

1.1 Begriffs-, Wertungs- und Kalkulationslogik

MUSS-Anforderungen sind zwingend zu erfüllen. Die Nichterfüllung einer MUSS-Anforderung kann zum Ausschluss des Angebots führen, soweit in den Vergabeunterlagen nichts Abweichendes geregelt ist.

SOLL-Anforderungen beschreiben qualitäts- oder bewertungsrelevante Anforderungen. Die Erfüllung, teilweise Erfüllung oder Nichterfüllung wird ausschließlich nach Maßgabe der Bewertungsmatrix bewertet.

Optionen sind separat auszuweisen und zu bepreisen. Optionen werden nur Vertragsbestandteil, soweit sie durch den Auftraggeber ausdrücklich beauftragt oder abgerufen werden. Soweit Optionen in die Angebotswertung einfließen, ergibt sich dies ausschließlich aus Preisblatt und Bewertungsmatrix.

Nachweise, Konzepte und Dokumentationen sind nur dann Zuschlags- oder Bewertungskriterien, wenn dies in den Vergabeunterlagen, der Bewertungsmatrix oder den Eignungskriterien ausdrücklich festgelegt ist. Im Übrigen dienen sie dem Nachweis der Leistungserfüllung und der späteren Vertragsdurchführung.

Grundleistungen sind in den angebotenen Pauschal-, Projekt- oder Betriebspreisen enthalten, soweit sie in dieser Leistungsbeschreibung nicht ausdrücklich als Option oder gesondert zu vergütende Leistung gekennzeichnet sind.

2. Rahmenbedingungen und Ausgangslage

2.1 Systemlandschaft

Der Faxdienst wird auf Avaya C3000 betrieben und zukünftig ohne Avaya Aura eingesetzt. Der Faxverkehr ist geschäftskritisch; derzeit werden ca. 60.000 Faxe pro Monat verarbeitet.

Die Faxlösung ist Teil der Kommunikationssysteme der AOK Niedersachsen, neben Microsoft Teams als Lösung für die Office-Telefonie sowie der sogenannten Omnikanalplattform, einer Omnichannel-Contact-Center-Lösung auf Basis von Amazon-Technologie.

2.2 Mail-Infrastruktur

Derzeit befindet sich die Mail-Infrastruktur im Hybridbetrieb (Exchange On-Premises / Exchange Online). Im Verlauf der Vertragslaufzeit erfolgt gegebenenfalls der vollständige Übergang auf Exchange Online (Microsoft 365).

Der Faxdienst ist aktuell in die Mail-Infrastruktur integriert (Fax-to-Mail / Mail-to-Fax) und so bereitzustellen, dass auch der Umstieg auf Exchange Online ohne zusätzliche Kosten sowie ohne technische Anpassungen durch den Auftraggeber unterstützt wird.

Der Faxversand aus Exchange/Microsoft 365 sowie über Multifunktionsgeräte (SMTP) ist sicherzustellen.

2.3 SIP-Trunk / SBC

Der SIP-Trunk wird durch den Auftraggeber bereitgestellt. Die Vertrags- und Kommunikationsbeziehung zum Provider verbleibt beim Auftraggeber. Die Eröffnung, Steuerung und Eskalation von Provider-Tickets erfolgt durch den Auftraggeber.

Der Auftragnehmer unterstützt im Störfall durch technische Vorqualifizierung, Analyse, Bereitstellung von SIP-/T.38-/G.711-Diagnosen, Logdaten, Fehlerbildern sowie durch Mitwirkung an der Ursachenabgrenzung.

Die Interoperabilität zum vom Auftraggeber bereitgestellten SBC/SIP-Trunk ist sicherzustellen. Erforderliche Ports, Protokolle, SIP-Parameter, T.38-/G.711-Einstellungen und Fehlerbilder werden im Rahmen der Inbetriebnahme abgestimmt und in der Betriebsdokumentation fixiert. Der erforderliche On-Premise Session Border Controller für die Anbindung des Faxservers C3000 wird parallel ausgeschrieben und ist nicht Bestandteil dieses Loses.

3. Technische Anforderungen und Systemarchitektur

Für Systemarchitektur und Hochverfügbarkeit ist ein technisches Konzept zu erstellen und mit dem Angebot abzugeben.

3.1 Architektur

Der Betrieb erfolgt in zwei Rechenzentren auf durch den Auftraggeber bereitgestellten Windows-Servern 2025. Der Auftragnehmer verantwortet den Betrieb der C3000-Applikationen.

Die Lösung umfasst mindestens folgende C3000-Funktionen bzw. Komponenten:

- UM-Server (zentrale Serverkomponente),
- Communication Gateway (Fax-Signalisierung, Faxkanäle),
- SMTP-Connector (Anbindung an Exchange / Microsoft 365),
- Reporting und Statistik,
- Web-Administration,
- Datenbank (Konfiguration, Benutzer und Statistikdaten).

3.2 Hochverfügbarkeit

Die Plattform ist über zwei Rechenzentren hochverfügbar bereitzustellen. Die Datenhaltung ist redundant auszugestalten, z. B. durch Spiegelung oder Replikation.

Im Ausfall eines Standortes übernimmt der verbleibende Standort die Vollast. Failover ist automatisiert oder mit minimalem Bedienereingriff innerhalb von ≤ 10 Minuten sicherzustellen. Das Hochverfügbarkeits- und Wiederherstellungskonzept einschließlich Testfällen ist zur Abnahme vorzulegen und jährlich im Rahmen dokumentierter Tests nachzuweisen.

3.3 Faxfunktionalität (C3000)

Für die Faxfunktionalität ist ein technisches Konzept zu erstellen und mit dem Angebot abzugeben.

3.3.1 Funktionen

Die Lösung muss mindestens folgende Funktionen bereitstellen:

- Fax-to-Mail (PDF verpflichtend, TIFF optional),
- Mail-to-Fax,
- Versand aus Exchange / Microsoft 365,
- Versand über Multifunktionsgeräte (SMTP),
- frei gestaltbare Deckblätter, Kopf- und Fußzeilen,
- Reporting und Controlling ein- und ausgehender Faxe mit mindestens 12 Monaten Vorhaltezeit,
- frei konfigurierbare Retry-Strategien.

3.3.2 Inhalte und Metadaten

Fax-E-Mails enthalten mindestens Absenderrufnummer, Zielrufnummer, Seitenanzahl und Zeitstempel.

Für gesendete Faxe ist ein Sendebericht zu erzeugen.

Die Aufnahme der ersten Seite in den Sendebericht muss konfigurierbar sein und erfolgt nur, soweit dies vom Auftraggeber ausdrücklich vorgegeben, fachlich erforderlich und datenschutzrechtlich zulässig ist.

3.3.3 Leistungskennzahlen (KPI)

Für den C3000-Faxserverdienst gelten mindestens folgende Leistungskennzahlen:

- Fax-Erfolgsquote $\geq 97\%$ monatlich innerhalb der Servicezeit,
- Protokollpräferenz T.38, Fallback G.711,
- SLA- und Betriebsberichte mit Aufschlüsselung nach Übertragungsprotokoll, Retry-Statistik, Fehlercodes, Durchsatz und Kapazitätsentwicklung.

4. Liefer- und Leistungsumfang

4.1 Abgrenzung Projektleistung / Betriebsleistung

Leistungen in diesem Kapitel betreffen primär einmalige oder projektbezogene Leistungen, insbesondere Übernahme, Implementierung, initiale Konfiguration, Migration, initiale Dokumentation, Tests und produktionsvorbereitende Maßnahmen.

Wiederkehrende Betriebsleistungen sind in Kapitel 5 beschrieben und im Betriebspreis zu kalkulieren, soweit nicht ausdrücklich anders geregelt.

Für den Leistungsumfang des Managed Service ist ein Betriebskonzept zu erstellen und mit dem Angebot abzugeben.

4.2 Projekt- und Übernahmeleistungen

Der Auftragnehmer erbringt insbesondere folgende Projekt- und Übernahmeleistungen:

- Unterstützung beim Betriebsübergang vom bisherigen Dienstleister,
- Übernahme, Prüfung und Stabilisierung der bestehenden C3000-Umgebung,
- Abstimmung der technischen Umsetzung mit dem Auftraggeber,
- Vorbereitung des Regelbetriebs,
- Erstellung bzw. Aktualisierung der initialen Betriebs- und Systemdokumentation,
- Abstimmung der Schnittstellen zu Mail-Infrastruktur, SIP-Trunk, SBC, Multifunktionsgeräten und Monitoring,
- Vorbereitung und Durchführung der Abnahme nach Testkatalog.

4.3 Provider-/SBC-Unterstützung (projektbezogen)

Der Auftragnehmer unterstützt bei Provider-/SBC-bezogenen Störungen und Inbetriebnahmethemen, insbesondere durch Analyse, Bereitstellung technischer Diagnosedaten und Mitwirkung an der Ursachenabgrenzung.

Die Vertrags-, Kommunikations- und Eskalationsbeziehung zum SIP-Trunk-Provider verbleibt beim Auftraggeber. Die Eröffnung, Steuerung und Eskalation von Provider-Tickets erfolgt durch den Auftraggeber.

5. Betrieb und Wartung (Managed Service)

5.1 Abgrenzung Regelbetrieb

Leistungen in diesem Kapitel betreffen den laufenden Regelbetrieb, insbesondere Betrieb, Wartung, Support, Monitoring, Störungsbearbeitung, Lifecycle-, Patch- und Release-Aktivitäten sowie die laufende Pflege der Betriebsdokumentation.

Einmalige Projektleistungen sind in Kapitel 4 beschrieben.

5.2 Betriebsleistungen

Der Auftragnehmer erbringt alle Leistungen zum sicheren und stabilen Betrieb der Systeme, insbesondere:

- 24×7-Monitoring aller relevanten System- und Dienstzustände einschließlich synthetischer Testfaxe ein- und ausgehend,
- Incident-, Problem-, Change- und Release-Management nach ITIL-orientierten oder vergleichbaren Prozessen,
- Patch- und Versionsmanagement für C3000-Komponenten und Betriebssysteme,
- regelmäßige Backups sowie mindestens jährlich dokumentierte Restore-Tests,
- Pflege einer vollständigen Betriebs- und Systemdokumentation,
- proaktives Zertifikats- und Kapazitätsmonitoring,
- monatliche Service-Meetings sowie regelmäßige technische Jour fixes,
- Supportanfragen via Ticket, E-Mail und Telefon,
- feste Ansprechpartner für technische und kaufmännische Belange,
- deutschsprachiger Support.

5.3 Wartung und Lifecycle Management

Der Auftragnehmer stellt die Wartung und den vollständigen Lifecycle-Betrieb des C3000-Faxserverdienstes sicher.

Dies beinhaltet insbesondere Patch- und Release-Management für C3000-Komponenten, Betriebssysteme, Datenbank, SMTP-Connector, Web-Administration und weitere betriebserforderliche Komponenten.

Weiter umfasst der Managed Service ein durchgängiges Schwachstellenmanagement, Konfigurationsversionierung, Zertifikatsmanagement sowie ein gesichertes Backup-/Restore-Konzept.

6. Service Level Agreement (SLA)

6.1 Vorbemerkung zum Geltungsbeginn der SLA

Die Regelungen dieses Kapitels (Servicezeiten, Reaktions-/Entstörzeiten, Verfügbarkeit & Messung, Sicherheits-/Compliance-KPIs sowie Service-Credits) gelten ab Go-Live gemäß dem im Projektplan bzw. Vergabekalender festgelegten Termin. Dies gilt auch für den Interimbetrieb bis zur vollständigen Abnahme des Faxserver-Dienstes.

6.2 Priorisierungsklassen P1/P2/P3

Die Priorisierung erfolgt anhand der betrieblichen Kritikalität des Faxservers und orientiert sich an branchenüblichen Modellen für zentrale Kommunikationssysteme.

P1 – Kritisch

Schwerwiegende Störung mit unmittelbarer Auswirkung auf den produktiven Faxbetrieb. Der Faxserver ist vollständig ausgefallen oder erheblich beeinträchtigt.

Beispiele:

- vollständiger Ausfall des Avaya C3000 Faxservers,
- keine Faxesendungen oder -empfänge möglich,
- Ausfall aller Faxkanäle,
- systemweite T.30/T.38-Fehler,
- Fax-Queue blockiert,
- zentrale Module oder Lizenzdienste ausgefallen.

Der geschäftliche Kommunikationsbetrieb per Fax ist massiv eingeschränkt oder nicht möglich.

P2 – Hoch

Teilfunktionseinschränkung mit spürbarer, aber nicht kritischer Beeinträchtigung des Betriebs.

Beispiele:

- Ausfall einzelner Faxkanäle oder Teilkomponenten,
- sporadische Übertragungsabbrüche,
- Störungen bei einzelnen Abteilungen,
- Probleme bei bestimmten Zielrufnummern oder Routen,
- Verzögerungen durch Teilmodule,
- fehlerhafte Verarbeitung einzelner Workflows.

Der Betrieb ist möglich, jedoch beeinträchtigt.

P3 – Normal

Nicht-kritische Störung oder Anfrage ohne unmittelbare Auswirkungen auf den operativen Faxbetrieb.

Beispiele:

- Konfigurationsanpassungen,
- Optimierungsanfragen,
- Logging-, Monitoring- oder Dokumentationsanfragen,
- geringfügige Anzeige- oder Komfortthemen,
- Nutzeradministration.

Der produktive Betrieb ist nicht beeinträchtigt.

6.3 Servicezeiten

Die Servicezeiten definieren die Zeitfenster, in denen der Auftragnehmer für Analyse, technische Vorqualifizierung und SLA-Reaktionszeiten zur Verfügung steht.

Während der Servicezeiten führt der Auftragnehmer die technische Vorqualifizierung und Analyse gemäß Priorisierung durch.

Die Koordination mit externen Providern (SIP-Trunk, Leitungen) erfolgt ausschließlich durch den Auftraggeber.

6.4 Reaktions- und Entstörzeiten

Die SLA-Zeiten gelten ausschließlich für Tätigkeiten im Verantwortungsbereich des Auftragnehmers.

P1 – Kritisch

- Reaktion: ≤ 15 Minuten,
- Workaround: ≤ 1 Stunde,
- Wiederherstellung: ≤ 2 Stunden, sofern im Verantwortungsbereich des Auftragnehmers.

P2 – Hoch

- Reaktion: ≤ 15 Minuten,
- Wiederherstellung: ≤ 4 Stunden.

P3 – Normal

- Reaktion: ≤ 2 Stunden,
- Wiederherstellung: ≤ 8 Stunden oder Umsetzung im nächsten regulären Wartungsfenster.

Liegt die Störungsursache außerhalb des Faxservers, z. B. Provider-Netz, PBX-Anbindung, SBC oder SIP-Leitung, unterstützt der Auftragnehmer durch technische Zuarbeit. Die Ticket-Eröffnung, Eskalation und Provider-Kommunikation obliegt dem Auftraggeber.

AT = Arbeitstag (Mo–Fr, niedersächsische Feiertage ausgenommen).

6.5 Verfügbarkeit & Messung

Monatliche Mindestverfügbarkeit Faxserver:

- ≥ 99,9 % (24×7).

Messpunkte:

- Serverdienst-Health,
- Faxkanalstatus,
- Queue-Laufzeiten und Verarbeitungsstatus,
- synthetische Testfaxe ein- und ausgehend,
- Modulverfügbarkeit,
- Datenbankverfügbarkeit,
- SMTP-Connector,
- Web-Administration,
- Replikations-/HA-Status.

Provider-bedingte Störungen werden separat ausgewiesen und nicht auf die SLA-Erfüllung angerechnet.

Verfügbarkeitsdefinition:

Verfügbarkeit [%] = ((Gesamtzeit – anrechenbare Ausfallzeit) / Gesamtzeit) × 100

Beispiel:

Wenn ein Monat 43.200 Minuten hat und es insgesamt 30 Minuten anrechenbare Ausfallzeit gab, ergibt sich:

$$((43.200 - 30) / 43.200) \times 100 = 99,93 \%$$

Ausnahmen, die nicht als Ausfallzeit gewertet werden:

- geplante Wartungen gemäß Kap. 8.3,
- durch den Auftraggeber veranlasste Änderungen oder Tests,
- höhere Gewalt,
- Provider-Störungen,
- Störungen durch vom Auftraggeber verantwortete Drittsysteme.

6.6 Service-Credits

Service Credits dienen der wirtschaftlichen Kompensation bei Leistungsabweichungen und stellen keinen Schadensersatz dar. Sie haben keinen rechtsvernichtenden oder beschränkenden Charakter gegenüber weitergehenden Ansprüchen des Auftraggebers. Service Credits dienen zudem der Qualitätssicherung und werden bei Nichterfüllung vereinbarter Service Level (SLA) fällig. Es handelt sich nicht um Vertragsstrafen, sondern um pauschalisierte Minderungsbeträge gemäß EVB IT Dienstvertrag. Die Service Credits werden monatlich berechnet und vom Monatsentgelt des betroffenen Services abgezogen. Die Gesamtsumme der Service Credits ist pro Monat auf maximal 15 % des Monatsentgelts begrenzt.

Weitergehende Rechte des Auftraggebers nach den EVB IT AGB sowie nach gesetzlichen Bestimmungen bleiben unberührt.

6.6.1 Auslöser für Service-Credits

Service-Credits werden ausgelöst durch:

- Unterschreiten der Verfügbarkeit (Messung gemäß 6.4)
- Überschreitung von Wiederherstellungszeiten (P1–P3) gemäß 6.3
- Nichtbereitstellung des monatlichen SLA-Berichts (vgl. 6.7)
- Unvollständige/verspätete RCA für P1/P2-Störungen
- Kumulierung: Credits aus mehreren Auslösern sind additiv (Deckelung siehe 6.6.5).

6.6.2 Staffel für Verfügbarkeits-Credits

(Monatlicher Messzeitraum; Definition und Ausnahmen gemäß 6.4)

Monatliche Verfügbarkeit	Minderungsbetrag
99,50 % bis < 99,90 %	5 %
99,00% bis < 99,50%	10 %
< 99,00%	15 %

6.6.3 Credits bei Verstoß gegen Wiederherstellungszeiten (p-basierte SLA)

Nur relevant für P1 und P2; P3 mit pauschaler Regel.

- P1 (kritisch): 1 % je begonnener Stunde Überschreitung; max. 5 % pro P1-Störung.
- P2 (hoch): 1 % je Überschreitung um > 1 Stunde; max. 2 % pro Störung.
- P3 (normal): 0,5 % pauschal ab > 4 Stunden Überschreitung; max. 1 % pro Störung.

6.6.4 Credits für Berichtswesen

Pflichtverletzung	Minderungsbetrag
Fehlender/verspäteter Monats-SLA-Bericht	1 %
Fehlende RCA zu P1/P2 innerhalb 1 Arbeitstag	1 %

6.6.5 Deckelung

Die monatliche Gesamtsumme aller Credits (Verfügbarkeit, P-basierte SLA-Verstöße, Reporting, Fax-Erfolgsquote) beträgt maximal 15 % des monatlichen Serviceentgelts.

6.6.6 Beispiele

Beispiel 1 – Verfügbarkeit unterschritten:

- Monatsentgelt: 12.000 €,
- gemessene Verfügbarkeit: 99,2 %,
- Staffel gemäß 6.6.2: 10 % Credit,
- Berechnung: $12.000 \text{ €} \times 10 \% = 1.200 \text{ € Credit}$.

Beispiel 2 – Fax-Erfolgsquote unterschritten:

- Fax-Erfolgsquote: 94,2 %,
- Staffel gemäß 6.6.3: 3 % Credit,
- Berechnung: $12.000 \text{ €} \times 3 \% = 360 \text{ € Credit}$.

Beispiel 3 – P1-Störung über SLA:

- SLA: Wiederherstellung ≤ 2 Stunden,
- tatsächlich: 5 Stunden,
- Überschreitung: 3 begonnene Stunden,
- Credit: 1 % je begonnene Stunde = 3 %,
- Berechnung: $12.000 \text{ €} \times 3 \% = 360 \text{ € Credit}$.

Gesamtbeispiel:

- Verfügbarkeit: 10 %,
- Fax-Erfolgsquote: 3 %,
- P1-SLA-Verstoß: 3 %,

- Summe: 16 %,
- wegen Deckelung maximal 15 %,
- Credit gesamt: 12.000 € × 15 % = 1.800 €.

6.6.7 Fax-Erfolgsquote („Fax Success Rate“)

Innerhalb der definierten Servicezeit, Monatsmittelwert:

- 95,00 % bis < 97,00 % = 1 %,
- 93,00 % bis < 95,00 % = 3 %,
- < 93,00 % = 5 %.

Credits aus der Fax-Erfolgsquote werden zusätzlich zu Verfügbarkeits- und SLA-Credits berechnet, unterliegen jedoch der monatlichen Gesamtkappung gemäß Kap. 6.6.5.

6.7 Reporting

Der Auftragnehmer erstellt für den C3000-Faxserverdienst einen monatlichen SLA- und Betriebsreport. Der Report dient der nachvollziehbaren Dokumentation der Servicequalität, der SLA-Erfüllung, der Betriebsstabilität, der Kapazitätsentwicklung sowie der für den Betrieb relevanten technischen und organisatorischen Ereignisse.

Der monatliche Report enthält mindestens Angaben zur Verfügbarkeit des Faxserverdienstes im jeweiligen Berichtszeitraum, zur Fax-Erfolgsquote, zur Anzahl und Priorisierung der Incidents nach P1, P2 und P3, zu Störungsursachen, Bearbeitungsständen, Wiederherstellungszeiten und gegebenenfalls bereitgestellten Workarounds.

Provider- oder drittssystembedingte Störungen sind gesondert auszuweisen und von durch den Auftragnehmer zu verantwortenden Störungen abzugrenzen.

Zusätzlich sind die technischen Betriebskennzahlen des Faxdienstes darzustellen. Hierzu gehören insbesondere:

- Aufschlüsselung nach T.38- und G.711-Übertragungen,
- Retry-Statistiken,
- häufige Fehlercodes,
- Durchsatz- und Lastentwicklung,
- Queue- und Verarbeitungsstatus,
- erkennbare Kapazitäts- oder Trendentwicklungen.

Soweit synthetische Testfaxe oder vergleichbare Monitoringmaßnahmen eingesetzt werden, sind deren Ergebnisse zusammenfassend darzustellen.

Der Report enthält ferner den Status relevanter Betriebs- und Sicherheitsnachweise, insbesondere Backup- und Restore-Status, Zertifikatsstatus, Patch- und Change-Status sowie datenschutz- oder auditrelevante Auffälligkeiten.

Administrations- und Auditinformationen sind datensparsam, zweckgebunden und ohne Offenlegung von Faxinhalten darzustellen, soweit eine Offenlegung nicht ausdrücklich erforderlich und durch den Auftraggeber freigegeben ist.

Service-Credits sind im Report transparent auszuweisen. Hierzu sind die auslösenden Ereignisse, die jeweilige Berechnungsgrundlage, die angewandte Staffel, Zwischensummen, die Anwendung der monatlichen Gesamtkappung sowie die resultierende Gutschrift nachvollziehbar darzustellen.

Der monatliche SLA- und Betriebsreport ist dem Auftraggeber spätestens bis zum fünften Arbeitstag des Folgemonats bereitzustellen, sofern nichts Abweichendes vereinbart ist. Die Bereitstellung erfolgt mindestens in einem menschenlesbaren Format, z. B. PDF, sowie auf Anforderung zusätzlich in einem strukturierten Format, z. B. Excel oder CSV.

Fehlende oder fehlerhafte Reportbestandteile sind nach Anzeige durch den Auftraggeber innerhalb von zwei Arbeitstagen nachzuliefern oder zu korrigieren. Die Verpflichtung zur Nachlieferung oder Korrektur lässt etwaige Service-Credits wegen verspäteter oder unvollständiger Berichterstattung unberührt.

Zusätzlich stellt der Auftragnehmer quartalsweise eine konsolidierte Betriebsübersicht mit Trendanalysen, Kapazitätsentwicklung, Security-/Zertifikatsstatus und Maßnahmenempfehlungen bereit.

6.8 Service-Credits, Messung und Verantwortungsgrenzen

Service-Credits sind pauschalisierte Minderungs- bzw. Gutschriftmechanismen für definierte SLA-Verstöße und ersetzen nicht die vereinbarten Incident-, Eskalations-, Mängel- oder sonstigen vertraglichen Rechte, soweit vertraglich nichts Abweichendes geregelt ist.

Die Berechnung von Service-Credits setzt eine nachvollziehbare Messung, Zuordnung und Dokumentation voraus. Messzeitraum, Messmethode, Datenquellen, Wartungsfenster, Ausschlüsse, Mitwirkungsverzug des Auftraggebers, Störungen durch vom Auftraggeber verantwortete Provider oder Drittsysteme sowie Fälle höherer Gewalt sind bei der Bewertung zu berücksichtigen.

SLA-Verstöße, deren Ursache außerhalb des Verantwortungsbereichs des Auftragnehmers liegt, lösen keine Service-Credits aus. Der Auftragnehmer hat in solchen Fällen die Ursache, Abgrenzung und Mitwirkungshandlungen nachvollziehbar zu dokumentieren.

7. Sicherheit und Compliance

7.1 Übergreifende Datenschutz- und Sicherheitsgrundsätze

Der Auftragnehmer hat die für den C3000-Faxserverdienst relevanten Datenschutz-, Informationssicherheits- und Betriebsanforderungen widerspruchsfrei in den jeweils geschuldeten Konzepten umzusetzen. Die Konzepte sind aufeinander abzustimmen und während der Vertragslaufzeit aktuell zu halten.

Aufgrund der möglichen Verarbeitung personenbezogener Daten und Sozialdaten im Sinne der §§ 67 ff. SGB X sind Faxinhalte, Faxmetadaten, Sendeberichte, Protokolle, Reporting-, Statistik-, Diagnose- und Backup-Daten zweckgebunden, datensparsam und zugriffsbeschränkt zu verarbeiten, soweit solche Daten betroffen sind.

Die Anzeige- und Prüfpflichten nach § 80 SGB X verbleiben beim Auftraggeber. Der Auftragnehmer unterstützt den Auftraggeber durch Bereitstellung der für die Anzeige, Prüfung und Dokumentation erforderlichen Informationen zu Leistung, Datenarten, technischen und organisatorischen Maßnahmen, Unterauftragnehmern und Weisungen.

7.2 Datenschutz durch Technikgestaltung, datenschutzfreundliche Voreinstellungen und Art. 32 DSGVO

Der Auftragnehmer unterstützt den Auftraggeber bei der Umsetzung der Grundsätze Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art. 25 DSGVO.

Systeme, Prozesse und Standardkonfigurationen sind so auszugestalten, dass Faxinhalte, Faxmetadaten, Sendeberichte, Protokoll-, Reporting-, Statistik-, Diagnose- und Backup-Daten nur verarbeitet werden, soweit dies für Betrieb, Sicherheit, Störungsanalyse, Nachweisführung, Auditierung oder vertragliche Leistungserbringung erforderlich ist.

Der Auftragnehmer setzt geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO um. Diese umfassen insbesondere Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit sowie regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen.

Faxinhalte dürfen im Rahmen von Betrieb, Test, Diagnose, Restore, Incident-Bearbeitung oder Übergabe nur verarbeitet oder offengelegt werden, soweit dies zwingend erforderlich und durch den Auftraggeber freigegeben oder vertraglich zugelassen ist.

7.3 Sicherheitskonzept

Der Auftragnehmer erstellt ein eigenständiges, systembezogenes Sicherheitskonzept für den C3000-Faxserverdienst.

Das Sicherheitskonzept beschreibt die sicherheitsrelevante Gesamtarchitektur, den Schutzbedarf sowie die grundlegenden Sicherheitsmaßnahmen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit. Es berücksichtigt einschlägige Normen und Standards, insbesondere ISO/IEC 27001 sowie BSI IT-Grundschutz, soweit diese auf die konkrete Systemumgebung anwendbar sind.

Das Sicherheitskonzept ist als übergeordnetes Rahmendokument auszugestalten. Es beschreibt die sicherheitsrelevanten Zusammenhänge zwischen Architektur, Betrieb, Zugriffsschutz, Protokollierung, Monitoring, Schwachstellenmanagement, Notfallvorsorge, Backup/Restore, Incident-Bearbeitung, Datenschutz und Exit.

Das Sicherheitskonzept ersetzt nicht die eigenständig zu liefernden Fachkonzepte. Insbesondere das Zugriffskonzept gemäß Kapitel 7.8 und Anlage 15.2.4 ist als eigenständiges Konzept zu erstellen. Das Sicherheitskonzept hat jedoch die Schnittstellen zu diesen Konzepten zu beschreiben und deren widerspruchsfreie Einbindung sicherzustellen.

Das Sicherheitskonzept umfasst mindestens folgende Inhalte:

7.3.1 Sicherheitsarchitektur und Systemdesign

- Beschreibung der sicherheitsrelevanten Gesamtarchitektur,
- Zonierung, Netzsegmentierung und Schutzmechanismen,
- Absicherung von Administrations-, SIP-/T.38-/G.711-, SMTP-, Datenbank- und Web-Administrationspfaden,
- Einbindung des Schnittstellenkonzepts gemäß Anlage 15.2.1.

7.3.2 Schnittstelle zum Zugriffskonzept und Identitätsmanagement

- Beschreibung der übergeordneten Anforderungen an Zugriffsschutz und Identitätsmanagement,
- Abgrenzung zum eigenständigen Zugriffskonzept gemäß Kapitel 7.8 und Anlage 15.2.4,
- Darstellung der sicherheitsrelevanten Anforderungen an administrative und privilegierte Zugriffe,
- Einbindung des Credentials- und Konfigurationsinventars gemäß Anlage 15.2.10.

7.3.3 Betriebssicherheit

- Einbindung des Betriebskonzepts gemäß Anlage 15.2.2,
- Härtung der eingesetzten Systeme und Komponenten,
- Einbindung des Schwachstellen- und Patchmanagement-Konzepts gemäß Anlage 15.2.15,
- Einbindung des Change- und Konfigurationsmanagement-Konzepts gemäß Anlage 15.2.16.

7.3.4 Protokollierung und Sicherheitsüberwachung

- Einbindung des Protokollierungs- und Audit-Konzepts gemäß Anlage 15.2.8,
- Einbindung des Monitoring- und Alarmierungskonzepts gemäß Anlage 15.2.7,
- Maßnahmen zur Sicherstellung der Nachvollziehbarkeit, Revisionsfähigkeit und manipulationsgeschützten Protokollierung administrativer Tätigkeiten.

7.3.5 Datensicherung und Wiederherstellung

- Einbindung des Backup- und Restore-Konzepts gemäß Anlage 15.2.9,
- Regelungen zur Sicherstellung der Datenverfügbarkeit und Datenintegrität,
- Durchführung und Dokumentation regelmäßiger Wiederherstellungstests.

7.3.6 Notfallmanagement und Wiederanlauf

- Einbindung des Notfall- und Wiederanlaufkonzepts gemäß Anlage 15.2.6,
- Maßnahmen zur Sicherstellung der Betriebsfortführung,
- Definition von Wiederanlaufzielen, insbesondere RTO und RPO, soweit einschlägig.

7.3.7 Behandlung von Sicherheitsvorfällen

- Einbindung des Incident-, Problem- und Eskalationskonzepts gemäß Anlage 15.2.12,
- Prozesse zur Erkennung, Meldung, Bewertung und Behandlung von Sicherheitsvorfällen,
- Melde- und Eskalationswege einschließlich Einbindung von Informationssicherheit und Datenschutz.

7.3.8 Qualitätssicherung und Tests

- Einbindung des Test- und Abnahmekonzepts gemäß Anlage 15.2.5,
- Durchführung sicherheitsrelevanter Tests, z. B. Schwachstellenanalysen oder Penetrationstests, soweit vereinbart,
- sicherheitsbezogene Abnahmekriterien und Nachweise.

7.3.9 Datenschutz und Compliance

- Einbindung des Nachweises zur Umsetzung von Privacy by Design und Privacy by Default gemäß Anlage 15.2.14,
- Darstellung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO,
- Berücksichtigung von Anforderungen aus Datenschutz, Informationssicherheit, Sozialdatenschutz und Compliance.

7.3.10 Dokumentation und Nachweisführung

- Einbindung des Dokumentationsindex / As-Built-Verzeichnisses gemäß Anlage 15.2.11,
- Sicherstellung der Vollständigkeit, Aktualität, Versionierung und Auditierbarkeit der Dokumentation.

7.3.11 Übergabe und Beendigung

- Einbindung des Übergabe- und Exit-Konzepts gemäß Anlage 15.2.13,
- Regelungen zur Datenrückgabe, Übertragung, Löschung oder Anonymisierung bei Vertragsende,
- Sicherstellung eines geordneten Übergangs des Betriebs.

Die Erstellung separater, inhaltlich redundanter Dokumente wird nicht erwartet. Ziel ist ein kohärentes Sicherheitskonzept mit klarer Referenzierung der eigenständigen bzw. ergänzenden Fachkonzepte.

Das Sicherheitskonzept ist während der Vertragslaufzeit fortzuschreiben und an veränderte technische, organisatorische oder rechtliche Rahmenbedingungen anzupassen. Änderungen sind nachvollziehbar zu versionieren und dem Auftraggeber vorzulegen.

7.4 System- und Betriebssystemhärtung

Für den Betrieb des Faxserversystems sind geeignete System- und Betriebssystemhärtungsmaßnahmen nach anerkanntem Stand der Technik umzusetzen.

Als Orientierung können BSI IT-Grundschutz, CIS Benchmarks oder vergleichbare herstellernerneutrale Sicherheitsbaselines herangezogen werden, soweit diese auf die eingesetzten Komponenten anwendbar sind.

Erforderliche Antivirus- oder Endpoint-Security-Ausschlüsse für C3000-spezifische Verzeichnisse, temporäre Arbeitsbereiche und Datenbankpfade sind nach Herstellervorgaben, Sicherheitsbewertung und Freigabe durch den Auftraggeber dokumentiert umzusetzen.

7.5 BSI-Bezug für SIP-/Faxkommunikationspfade

Für die Absicherung der SIP-, T.38-/G.711-, Faxkommunikations- und Administrationspfade sind die einschlägigen Anforderungen und Empfehlungen des BSI zu berücksichtigen, soweit diese auf die eingesetzten Kommunikationspfade und die konkrete Architektur anwendbar sind.

Dies umfasst insbesondere eine Orientierung am IT-Grundschutz-Baustein NET.4.2 VoIP sowie, soweit einschlägig, am BSI-Kompendium für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf (KomTK).

Eine vollständige Umsetzung einzelner BSI-Kompendien oder Bausteine ist nur geschuldet, soweit dies in dieser Leistungsbeschreibung ausdrücklich gefordert oder vom Auftraggeber im Rahmen der Konzepte vorgegeben wird.

7.6 IT-Service-Management, KRITIS-, NIS-2-/BSIG- und vergleichbare Anforderungen

Die Betriebsprozesse orientieren sich an etablierten IT-Service-Management-Prinzipien, insbesondere ITIL-orientierten oder vergleichbaren Prozessen.

Eine bestimmte ITIL-Zertifizierung des Auftragnehmers wird hierdurch nicht begründet, soweit sie nicht ausdrücklich an anderer Stelle gefordert ist.

Soweit der Auftraggeber, der Dienst oder die betroffenen Systeme gesetzlichen Anforderungen aus KRITIS-, NIS-2-/BSIG- oder vergleichbaren Vorgaben unterliegen, sind die hieraus resultierenden Anforderungen nach Vorgabe des Auftraggebers zu berücksichtigen. Der Auftragnehmer unterstützt den Auftraggeber hierbei durch die geschuldeten Nachweise, Konzepte, Meldungen und Mitwirkungsleistungen.

7.7 Vorhalte- und Löschfristen

Betriebs-, Sicherheits-, Audit-, Protokoll-, Reporting-, Statistik- und Nachweisdaten, die personenbezogene Daten oder Sozialdaten enthalten können, sind zweckgebunden nur solange vorzuhalten, wie dies für Betrieb, Störungsanalyse, Sicherheitsnachweis, Auditierung, Nachvollziehbarkeit von Faxübertragungen oder vertragliche Nachweispflichten erforderlich ist. Soweit eine Aufbewahrung von mindestens 12 Monaten vorgesehen ist, gilt ergänzend eine maximale Vorhaltefrist von 36 Monaten für Audit-, Nachweis- und Reportingdaten.

Faxinhalte, Diagnoseexporte, Detailprotokolle, Testdaten mit Inhaltsbezug und vergleichbare Detaildaten sind nur anlassbezogen, zweckgebunden, zugriffsbeschränkt und so kurz wie möglich vorzuhalten. Die maximale Vorhaltefrist von 36 Monaten gilt nicht als Regelfrist für solche Detaildaten.

7.8 Zugriffskonzept

Der Auftragnehmer erstellt ein eigenständiges Zugriffskonzept für den C3000-Faxserverdienst. Das Zugriffskonzept beschreibt die konkrete Ausgestaltung der Zugriffsmöglichkeiten auf Systeme, Administrationsoberflächen, Schnittstellen, Protokolle, Reports, Monitoringdaten, Konfigurationsdaten, Faxmetadaten, Statistikdaten, Diagnoseinformationen, Backup-Daten und sonstige betriebsrelevante Informationen.

Das Zugriffskonzept umfasst insbesondere:

- Rollen- und Berechtigungsmodelle,
- administrative und privilegierte Zugriffe,
- Rollen nach dem Prinzip der minimal erforderlichen Berechtigungen,
- Mehr-Faktor-Authentifizierung, soweit technisch möglich und für die eingesetzten Komponenten verfügbar,
- Vier-Augen-Prinzip für kritische administrative Tätigkeiten,
- personenbezogene Read-Only-Zugänge des Auftraggebers,
- Zugriffsmöglichkeiten des Auftraggebers für Review, Audit, Monitoring und Fehleranalyse,
- Regelungen zu nicht-invasiven Diagnosehandlungen,
- Rezertifizierung von Berechtigungen,

- Entzug und Änderung von Berechtigungen,
- Protokollierung und Nachvollziehbarkeit administrativer Zugriffe,
- Umgang mit Service-, Funktions- und Notfallkonten,
- Abgrenzung zwischen Auftraggeber, Auftragnehmer, Hersteller, bisherigem Betreiber und sonstigen Dritten.

Das Zugriffskonzept ist eigenständig zu erstellen und als Anlage 15.2.4 vorzulegen. Es ist mit dem Sicherheitskonzept gemäß Kapitel 7.3 und Anlage 15.2.3 sowie mit dem Protokollierungs- und Audit-Konzept gemäß Anlage 15.2.8 widerspruchsfrei abzustimmen.

Zugriffe auf personenbezogene Daten, Sozialdaten, Faxinhalte, Faxmetadaten, Sendeberichte, Diagnoseinformationen, Protokolle und vergleichbare Detaildaten dürfen nur zweckgebunden, rollenbasiert, datensparsam und nachvollziehbar protokolliert erfolgen.

8. Monitoring, Wartungsfenster und Protokollierung

8.1 Monitoring- und Alarmierungskonzept

Der Auftragnehmer erstellt ein Monitoring- und Alarmierungskonzept.

Das Konzept beschreibt die zu überwachenden technischen, betrieblichen und sicherheitsrelevanten Parameter, Monitoring-Schnittstellen, Alarmierungslogik, Schwellenwerte, Ticket- bzw. Ereigniserzeugung sowie Benachrichtigungs- und Eskalationswege.

Das Monitoring umfasst mindestens:

- C3000-Komponenten,
- UM-Server,
- Communication Gateway,
- SMTP-Connector,
- Datenbank,
- Web-Administration,
- Faxkanäle,
- Queue- und Verarbeitungsstatus,
- Fax-to-Mail- und Mail-to-Fax-Funktionalität,
- synthetische Testfaxe,
- Zertifikate,
- Systemressourcen,
- Backup-/Restore-Status,
- Replikations-/HA-Status,
- administrative Zugriffe.

8.2 Protokollierungs- und Audit-Konzept

Der Auftragnehmer erstellt ein Protokollierungs- und Audit-Konzept.

Administrative und privilegierte Zugriffe sind vollständig, manipulationsgeschützt und nachvollziehbar zu protokollieren und müssen durch den Auftraggeber auswertbar sein. Die Schutzmechanismen für Log- und Protokolldateien sind darzustellen.

Faxinhalte dürfen nicht standardmäßig in Protokollen, Reports, Diagnoseexporten oder Sendeberichten verarbeitet oder gespeichert werden, soweit dies nicht ausdrücklich erforderlich, vertraglich geregelt oder durch den Auftraggeber freigegeben ist.

Faxmetadaten, Sendeberichte und Auswertungen sind datensparsam zu konfigurieren und möglichst aggregiert bereitzustellen.

8.3 Wartungsfenster und Notfall-Changes

Reguläre Wartungsfenster sind mit dem Auftraggeber abzustimmen, fristgerecht anzukündigen und im Reporting auszuweisen.

Notfall-Changes sind nur bei dringender betrieblicher oder sicherheitsrelevanter Erforderlichkeit zulässig und nachträglich vollständig zu dokumentieren.

9. Abnahme

Die Abnahme umfasst mindestens folgende Prüfpunkte:

- funktionale Übergabe inkl. Protokoll mittels Testkatalog,
- Fax-to-Mail,
- Mail-to-Fax,
- Sendebericht; Aufnahme der ersten Seite nur gemäß Kap. 3.3.2,
- Mitwirkung beim Betriebsübergang vom bisherigen Dienstleister,
- Test von Failover- und Wiederherstellungsszenarien,
- RZ-Wechsel,
- DB-Failover,
- Queue- und Verarbeitungsstatus,
- SMTP-Connector,
- Communication Gateway,
- Reporting,
- Monitoring und synthetische Testfaxe,
- Backup-/Restore-Nachweis,
- Sicherheits- und Zugriffsnachweise.

Konzeptunterlagen:

- Schnittstellenkonzept – vorgelegt, geprüft, freigegeben,
- Betriebskonzept – vorgelegt, geprüft, freigegeben,
- Sicherheitskonzept – vorgelegt, geprüft, freigegeben,
- Zugriffskonzept – vorgelegt, geprüft, freigegeben,
- Schwachstellen- und Patchmanagement-Konzept – vorgelegt, geprüft, freigegeben,
- Change- und Konfigurationsmanagement-Konzept – vorgelegt, geprüft, freigegeben,
- Test- und Abnahmekonzept – vorgelegt, geprüft, freigegeben,
- Notfall- und Wiederanlaufkonzept – vorgelegt, geprüft, freigegeben,
- Monitoring- und Alarmierungskonzept – vorgelegt, geprüft, freigegeben,
- Protokollierungs- und Audit-Konzept – vorgelegt, geprüft, freigegeben,
- Backup- und Restore-Konzept – vorgelegt, geprüft, freigegeben,
- Incident-, Problem- und Eskalationskonzept – vorgelegt, geprüft, freigegeben,
- Übergabe- und Exit-Konzept – vorgelegt, geprüft, freigegeben.

Der SLA-Start erfolgt ab Go-Live gemäß dem im Projektplan bzw. Vergabekalender festgelegten Termin.

9.1 Abnahmekatalog und objektive Prüfbarkeit

Der Auftragnehmer hat die Abnahme anhand eines mit dem Auftraggeber abgestimmten Abnahmekatalogs vorzubereiten und durchzuführen.

Der Abnahmekatalog enthält Testfälle, Erfolgskriterien, Nachweise, Abweichungen, Mängelklassen, Nachtestverfahren und Freigabeschritte.

Die Abnahme setzt eine nachvollziehbare Dokumentation der Testergebnisse, der technischen Nachweise und der offenen Punkte voraus. Teilabnahmen sind zulässig, soweit sie im Abnahmeprotokoll eindeutig abgegrenzt und vom Auftraggeber freigegeben werden.

9.2 Datenschutzkonforme Test- und Abnahmehandlungen

Test- und Abnahmehandlungen sind so zu planen und durchzuführen, dass personenbezogene Daten und Sozialdaten im Sinne der §§ 67 ff. SGB X nur verarbeitet werden, soweit dies für die jeweilige Test- oder Abnahmehandlung erforderlich ist.

Produktive Faxinhalte, Faxmetadaten, Sendeberichte oder sonstige produktive Sozialdaten dürfen nur verarbeitet oder offengelegt werden, soweit dies zwingend erforderlich und durch den Auftraggeber freigegeben ist.

Synthetische oder anonymisierte Testdaten sind vorrangig zu verwenden.

10. Rollen, Abgrenzung, Mitwirkung

Für Rollen und Abgrenzung ist ein Betriebskonzept zu erstellen und mit dem Angebot abzugeben.

10.1 Auftragnehmer (AN)

Der Auftragnehmer übernimmt insbesondere:

- Betrieb der Systeme inklusive Monitoring, Entstörung und technischer Koordination innerhalb des Verantwortungsbereichs des Auftragnehmers
- Administration, Patch und Release Management der C3000 Lösung einschließlich der hierfür durch den Auftraggeber bereitgestellten Windows Server sowie Zertifikats, Schlüssel und Kapazitätsmanagement.
- technische Vorqualifizierung und Zuarbeit bei Provider-/SBC-bezogenen Störungen,
- Pflege der Dokumentation,
- Zertifikats- und Kapazitätsmanagement,
- Patch- und Release-Management,
- Pflege und Aktualisierung der geschuldeten Konzepte,
- Erstellung von SLA- und Betriebsberichten,
- Benennung eines Servicemanagers,
- Benennung eines Technical Lead,
- Bereitstellung eines festen Technikerteams,
- deutschsprachigen Support.

Die Provider-Ticketsteuerung verbleibt beim Auftraggeber.

10.2 Auftraggeber (AG)

Der Auftraggeber übernimmt insbesondere:

- Fachadministration (Benutzer, Rufnummern),
- Bereitstellung der Infrastruktur einschließlich physischer bzw. virtueller Server, Betriebssystemlizenzen, Netzwerk, IP Ranges und Firewall Freigaben. Die Administration, Wartung und das Patchmanagement der bereitgestellten Windows Server erfolgen durch den Auftragnehmer.
- Bereitstellung SIP-Trunk,
- Bereitstellung Mail-Infrastruktur,
- Bereitstellung bzw. Betrieb von Sonderendpunkten, z. B. Multifunktionsgeräte,
- Provider-Kommunikation und Provider-Ticketsteuerung,
- Freigabe von Wartungsfenstern,
- Bereitstellung erforderlicher Ansprechpartner,
- lesende Berechtigungen für die gesamte Infrastruktur C3000 einschließlich Reporting und Monitoring.

11. Optionen

Optionale Leistungen sind gesondert auszuweisen und zu bepreisen.

Optionen sind insbesondere:

- Stundensatz Techniker, z. B. für Projekte und Weiterentwicklungen,
- Stundensatz Projektleiter, z. B. für Projekte und Weiterentwicklungen,
- Rufbereitschaft außerhalb der Regelzeiten,
- Change-Kontingente, z. B. 6–8 Stunden pro Monat,
- erweitertes Monitoring / SIP-Tracing,
- optionale Voice-Sprachboxen / Anrufbeantworter-Funktionalität, sofern durch den Auftraggeber abgerufen.

11.1 Preisblatt- und Optionslogik

Optionen sind im Preisblatt getrennt auszuweisen. Je Option sind Leistungsinhalt, Mengeneinheit, Preis, Abrufvoraussetzung und etwaige Mindest- oder Höchstmengen transparent darzustellen.

Optionen werden nur bei ausdrücklichem Abruf durch den Auftraggeber Vertragsbestandteil. Soweit eine Option in die Angebotswertung einbezogen wird, ergibt sich dies aus Bewertungsmatrix und Preisblatt.

Für optionale Zusatzleistungen sind insbesondere Tagessätze oder Stundensätze, Rufbereitschaft, Change-Kontingente, zusätzliche Betriebsleistungen, Exit-Unterstützung und sonstige Zusatzaufwände getrennt auszuweisen, soweit diese Leistungen angeboten oder gefordert werden.

12. Governance, Change und übergreifende Betriebssteuerung

12.1 Rollen und Gremien

Rollen, Gremien, Abstimmungswege und Verantwortlichkeiten ergeben sich aus den Rollen-, Mitwirkungs-, Change- und Governance-Regelungen dieser Leistungsbeschreibung.

12.2 Schwachstellen-, Patch-, Change- und Konfigurationsmanagement

12.2.1 Schwachstellen- und Patchmanagement

Der Auftragnehmer erstellt ein Konzept für das Schwachstellen- und Patchmanagement. Dieses beschreibt die Prozesse zur kontinuierlichen Identifikation, Bewertung und Priorisierung von Schwachstellen sowie zur zeitgerechten Planung, Bereitstellung, Prüfung und Installation von Sicherheitsupdates und Patches.

Das Konzept beschreibt insbesondere:

- Verantwortlichkeiten und Rollen,
- Quellen und Verfahren zur Schwachstellenidentifikation,
- Bewertung und Priorisierung von Schwachstellen in Abhängigkeit von Kritikalität und Schutzbedarf,
- Reaktions- und Umsetzungszeiten in Abhängigkeit von der Kritikalität,
- eingesetzte Werkzeuge und Informationsquellen,
- Test- und Freigabeverfahren vor produktiver Umsetzung,
- Dokumentation, Nachverfolgung und Reporting der Maßnahmen,
- Eskalationswege bei kritischen Schwachstellen oder Verzögerungen.

Das Schwachstellen- und Patchmanagement ist mit dem Sicherheitskonzept, dem Betriebskonzept, dem Change- und Konfigurationsmanagement sowie dem Incident-, Problem- und Eskalationskonzept abzustimmen.

Auswirkungen auf Datenschutz, Informationssicherheit, Verfügbarkeit, Schnittstellen, Faxinhalte, Faxmetadaten und Betrieb sind bei Bewertung, Priorisierung, Planung und Umsetzung von Sicherheitsupdates und Patches zu berücksichtigen.

12.2.2 Change- und Konfigurationsmanagement

Der Auftragnehmer erstellt ein Konzept für das Change- und Konfigurationsmanagement. Dieses beschreibt die kontrollierte Planung, Bewertung, Freigabe, Umsetzung und Dokumentation von Änderungen an Systemen, Konfigurationen, Schnittstellen und Betriebsprozessen.

Das Konzept beschreibt insbesondere:

- Verfahren zur Beantragung, Bewertung und Freigabe von Changes,

- Klassifizierung von Changes nach Risiko, Dringlichkeit und Auswirkung,
- Test- und Freigabeprozesse vor produktiver Umsetzung,
- Rollback- und Fallback-Verfahren,
- Dokumentation und Versionierung von Konfigurationen,
- Pflege eines aktuellen und vollständigen Konfigurationsinventars,
- Nachvollziehbarkeit von Änderungen,
- Einbindung des Auftraggebers bei freigabepflichtigen Änderungen,
- Umgang mit Notfall-Changes.

Änderungen sind nachvollziehbar zu beantragen, zu bewerten, freizugeben, umzusetzen und zu dokumentieren.

Auswirkungen auf Datenschutz, Informationssicherheit, Verfügbarkeit, Schnittstellen, Faxinhalte, Faxmetadaten, Sendeberichte, Datenbank, SMTP-Connector, Communication Gateway und Betrieb sind im Change-Verfahren zu berücksichtigen.

Das Change- und Konfigurationsmanagement ist mit dem Sicherheitskonzept, dem Zugriffskonzept, dem Betriebskonzept, dem Protokollierungs- und Audit-Konzept sowie dem Credentials- und Konfigurationsinventar abzustimmen.

12.3 Disaster-Recovery-Übungen

Disaster-Recovery- und Wiederanlaufübungen sind nach Maßgabe des Notfall- und Wiederanlaufkonzeptes gemäß Kap. 12.5 sowie der vereinbarten Betriebsprozesse zu planen, durchzuführen und zu dokumentieren.

12.4 Backup- und Restore-Konzept

Der Auftragnehmer erstellt ein Backup- und Restore-Konzept.

Das Konzept beschreibt Art, Umfang, Häufigkeit, Speicherorte, Schutzmaßnahmen, Verantwortlichkeiten, Wiederherstellungsverfahren, Testintervalle, Nachweise und Löschregelungen der Sicherungen.

Backup-Daten sind wegen möglicher personenbezogener Daten und Sozialdaten im Sinne der §§ 67 ff. SGB X besonders gegen unbefugten Zugriff, Veränderung, Verlust und unzulässige Offenlegung zu schützen.

Restore-Tests und Wiederherstellungsübungen sind regelmäßig, mindestens jährlich, durchzuführen und zu dokumentieren.

Dabei ist nachzuweisen, dass die für den Betrieb erforderlichen Konfigurations-, Zertifikats-, Datenbank-, System- und C3000-Daten innerhalb der vorgesehenen Wiederherstellungsprozesse vollständig und funktionsfähig wiederhergestellt werden können. Produktive Faxinhalte und produktive Sozialdaten sind hierbei zu vermeiden, soweit dies fachlich möglich ist.

Soweit fachlich sinnvoll, können Restore-Tests und Wiederherstellungsübungen mit Notfall- und Wiederanlaufübungen gemäß Kapitel 12.5 kombiniert werden.

Die Ergebnisse der Übungen sind auszuwerten. Erkannte Abweichungen, Risiken oder Verbesserungsmaßnahmen sind zu dokumentieren und in die Fortschreibung des Backup- und Restore-Konzeptes sowie gegebenenfalls des Notfall- und Wiederanlaufkonzeptes aufzunehmen.

12.5 Notfall- und Wiederanlaufkonzept

Der Auftragnehmer erstellt ein Notfall- und Wiederanlaufkonzept.

Maßnahmen zur Hochverfügbarkeit sind Bestandteil des Konzeptes, insbesondere:

- Hochverfügbarkeitsarchitektur,
- RZ-Wechsel,
- DB-Failover,
- Wiederanlaufreihenfolgen,
- C3000-Komponenten,
- Communication Gateway,
- SMTP-Connector,
- Datenbank,

- Web-Administration,
- Faxkanäle,
- Queue- und Verarbeitungsstatus,
- SIP-/T.38-/G.711-Kommunikationspfade.

Das Notfall- und Wiederanlaufkonzept beschreibt insbesondere Rollen und Verantwortlichkeiten, Auslösekriterien, Wiederanlaufprioritäten, Abhängigkeiten, technische Wiederherstellungsschritte, Kommunikationswege, Eskalationswege, Dokumentationspflichten sowie die Einbindung des Auftraggebers.

Notfall- und Wiederanlaufübungen sind regelmäßig, mindestens jährlich, zu planen, durchzuführen und zu dokumentieren.

Soweit fachlich sinnvoll, können diese Übungen mit Restore-Tests und Wiederherstellungsübungen gemäß Kapitel 12.4 kombiniert werden.

Die Ergebnisse der Übungen sind auszuwerten. Erkannte Abweichungen, Risiken oder Verbesserungsmaßnahmen sind zu dokumentieren und in die Fortschreibung des Notfall- und Wiederanlaufkonzeptes sowie gegebenenfalls des Backup- und Restore-Konzeptes aufzunehmen.

12.6 Incident-, Problem- und Eskalationskonzept

Der Auftragnehmer erstellt ein Incident-, Problem- und Eskalationskonzept.

Ein Incident ist jede ungeplante Unterbrechung oder Qualitätsminderung des Faxserverdienstes. Ziel des Incident-Managements ist die schnellstmögliche Wiederherstellung des vereinbarten Betriebszustands.

Ein Problem ist die zugrunde liegende oder potenzielle Ursache eines oder mehrerer Incidents. Das Problem-Management umfasst insbesondere Ursachenanalyse, Maßnahmenplanung und nachhaltige Fehlervermeidung.

Das Konzept beschreibt die Abgrenzung zwischen Incident und Problem, Kriterien für die Überführung eines Incidents in das Problem-Management, Eskalationsstufen, Verantwortlichkeiten, Kommunikationswege, Fristen, Dokumentation und Nachverfolgung. Für Incidents sind Eskalationsstufen festzulegen, einschließlich operativer Bearbeitung, technischer Eskalation, Einbindung des Auftraggebers, Management-Eskalation sowie Einbindung von Informationssicherheit und Datenschutz, soweit erforderlich.

Die technische Incident-Bearbeitung ersetzt nicht die datenschutzrechtliche Bewertung und Meldung eines Datenschutzvorfalls. Gleiches gilt für die Bewertung und Meldung von Informationssicherheitsvorfällen.

12.7 Übergabe- und Exit-Konzept

Der Auftragnehmer erstellt ein Übergabe- und Exit-Konzept.

Das Konzept beschreibt die geordnete Übergabe, Rückführung oder Migration des Faxdienstes an den Auftraggeber, einen Nachfolgedienstleister oder eine vom Auftraggeber benannte Stelle bei Vertragsende, Betreiberwechsel, Teilkündigung oder sonstiger Beendigung der Leistungserbringung.

Die Erstellung und Aktualisierung des Übergabe- und Exit-Konzeptes ist Bestandteil der Grundleistung.

Operative Exit-Unterstützung ist im Preisblatt gesondert als Personentag oder vergleichbare Mengeneinheit auszuweisen, soweit sie über die reine Konzeptpflege und Standarddokumentation hinausgeht.

Faxinhalte, Faxmetadaten, Sendeberichte, Protokolle, Reports, Statistikdaten, Diagnoseinformationen, Backup-Daten und sonstige im Rahmen des Betriebs verarbeitete Daten sind nach Weisung des Auftraggebers zurückzugeben, zu übertragen, zu löschen oder zu anonymisieren.

Die Löschung bzw. Rückgabe ist nachvollziehbar zu dokumentieren und auf Verlangen des Auftraggebers nachzuweisen.

13. Zeitplan und Meilensteine

Zeitplan und Meilensteine richten sich nach den Ausschreibungs-, Projekt- und Abnahmevorgaben des Auftraggebers.

Der Auftragnehmer erstellt nach Zuschlag einen detaillierten Projekt-, Integrations- und Cutover-Plan einschließlich Test-, Abnahme-, Fallback- und Kommunikationsplanung. Die Terminierung der Konzeptvorlagen, Freigaben, Integrationstests und Abnahmen erfolgt auf Basis eines zwischen Auftraggeber und Auftragnehmer abgestimmten Projektplans. Maßgeblich sind die im Projektplan festgelegten Fristen relativ zum verbindlich festgelegten Go-Live-Termin.

Abweichungen, Risiken und Terminänderungen sind frühzeitig anzuzeigen und im Projektstatus nachvollziehbar zu dokumentieren.

Der Vertragsbeginn ist für den 01.08.2026 vorgesehen. Projekt-, Übernahme-, Go-Live- und Regelbetriebstermine richten sich im Übrigen nach dem Vergabekalender sowie dem zwischen Auftraggeber und Auftragnehmer abgestimmten Projekt-, Integrations- und Cutover-Plan.

14. Vergaberechtskonforme Begründung (informativ)

Dieses Kapitel ist rein informativ und begründet keine eigenständigen Leistungspflichten des Auftragnehmers.

Verbindlich sind die Leistungsanforderungen, Vertragsunterlagen, Bewertungsmatrix, Eignungskriterien und Preisblätter der Vergabeunterlagen.

Vergaberechtliche Erwägungen, insbesondere Begründungen zu Produkt- oder Bestandsbezügen, sind vorrangig im Vergabevermerk bzw. in der Vergabeakte zu dokumentieren.

Der Bezug auf Avaya C3000 erfolgt aufgrund der vorhandenen Systemumgebung des Auftraggebers und der ausgeschriebenen Betriebs-, Wartungs- und Weiterführungsleistung. Gegenstand dieses Loses ist nicht die produktneutrale Neubeschaffung eines Faxserversystems, sondern der Managed Service für die bestehende C3000-Umgebung.

15. Anhänge

15.1 Anhänge (bereitgestellt durch den Auftraggeber)

- 15.1.1 Abnahmekatalog / Detail-Testfälle
- 15.1.2 Abnahmeprotokoll
- 15.1.3 Bewertungsmatrix
- 15.1.4 Preisblatt / Optionen
- 15.1.5 SLA-Report-Template

15.2 Anhänge (vom Auftragnehmer zu liefern / im Projektverlauf)

- 15.2.1 Schnittstellenkonzept
- 15.2.2 Betriebskonzept
- 15.2.3 Sicherheitskonzept
- 15.2.4 Zugriffskonzept
- 15.2.5 Test- und Abnahmekonzept
- 15.2.6 Notfall- und Wiederanlaufkonzept
- 15.2.7 Monitoring- und Alarmierungskonzept
- 15.2.8 Protokollierungs- und Audit-Konzept

- 15.2.9 Backup- und Restore-Konzept
- 15.2.10 Credentials- und Konfigurationsinventar
- 15.2.11 Dokumentationsindex / As-Built-Verzeichnis
- 15.2.12 Incident-, Problem- und Eskalationskonzept
- 15.2.13 Übergabe- und Exit-Konzept
- 15.2.14 Nachweis zur Umsetzung von Privacy by Design und Privacy by Default
- 15.2.15 Schwachstellen- und Patchmanagement-Konzept
- 15.2.16 Change- und Konfigurationsmanagement-Konzept

Die Konzepte gemäß 15.2.15 und 15.2.16 können als eigenständige Anlagen oder als eindeutig abgegrenzte Bestandteile des Sicherheitskonzeptes gemäß 15.2.3 geliefert werden. Inhaltliche Dopplungen sind zu vermeiden; die Konzepte sind widerspruchsfrei aufeinander abzustimmen.

Das Zugriffskonzept gemäß 15.2.4 ist ein eigenständiges Konzept und nicht lediglich Bestandteil des Sicherheitskonzeptes. Es ist jedoch mit dem Sicherheitskonzept, dem Protokollierungs- und Audit-Konzept sowie dem Credentials- und Konfigurationsinventar inhaltlich abzustimmen.