

EVB-IT-Dienstleistungsvertrag

Leistungsbeschreibung – Managed Service „Software Session Border Controller (SBC)“

Version: 1.4

Datum: 22.05.2026

1. Ziel und Gegenstand der Leistung

Gegenstand dieser Ausschreibung ist der Abschluss eines EVB-IT-Dienstleistungsvertrages über Beschaffung (Lizenz), Installation, Betrieb, Wartung und technische Betreuung eines softwarebasierten Session Border Controllers (SBC).

Der auszuschreibende SBC wird ausschließlich innerhalb der Systemumgebung des Auftraggebers (AG) betrieben und ist logisch wie physisch hinter dem vom Telekommunikationsanbieter bereitgestellten SBC positioniert.

Der auszuschreibende SBC erweitert die bestehende interne Infrastruktur in Bezug auf Türfreisprecheinrichtung, SIP-Telefone und Faxserver und ist Bestandteil unserer Microsoft Teams Systemlandschaft. Eine Interoperabilität mit der bestehenden Teams-Umgebung ist sicherzustellen; Microsoft Teams Direct Routing ist nicht Vertragsgegenstand. Der Einsatz erfolgt herstellerneutral; eine Anbieter- oder Plattformbindung ist nicht beabsichtigt.

Die Anbindung an das öffentliche Telefonnetz erfolgt ausschließlich über den beim Provider terminierenden SIP-Trunk des AG; der auszuschreibende SBC stellt weder eigene Carrier- noch Netzabschlussfunktionen bereit und nutzt keinen eigenen SIP-Trunk.

Der SBC dient der absichernden, steuernden und vermittelnden Anbindung folgender Dienste und Endpunkte innerhalb der Systemlandschaft des AG:

- Faxdienst C3000 – ausschließlich als SBC-seitige Schnittstelle (der Betrieb des C3000-Applikationsservers ist nicht Bestandteil dieser Ausschreibung)
- Sonderendpunkte: ausgewählte SIP-Telefone und Türfreisprecheinrichtungen (TFE)
- Weiterleitung (Transit) ausgewählter 0800-Service Rufnummern an einen externen Carrier/Dienstleister (Omnikanalplattform)
- Anbindung einer Outbound Call Center Lösung (ttCall - Hersteller ttUnited)

Nicht Gegenstand der Leistung sind insbesondere: Office-Telefonie, Unified-Communications-Funktionen, Contact-Center-Funktionen, Microsoft Teams Direct Routing als Nutzungsszenario, Endgeräteelieferungen sowie der Betrieb und Support des C3000-Applikationsservers.

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 auszuschreibende SBC wird im Rechenzentrumsumfeld des AG betrieben und übernimmt ohne eigene Trunk-Terminierung die interne Signalisierungs- und Medienverarbeitung für C3000, die definierten Sonderendpunkte/TFE sowie den 0800-Transitpfad. Die SIP-Trunk-Terminierung erfolgt ausschließlich am Provider-SBC des Telekommunikationsanbieters. Der auszuschreibende SBC wird über diesen Übergabepunkt angebunden.

2.2 Plattform & Architektur

- Bare-Metal-Installation (ohne Virtualisierung) auf Windows Server 2025 auf physischer Serverhardware des AG.
- Parallele Bereitstellung in zwei Rechenzentren (2 RZ): je ein Server pro RZ, Betrieb aktiv/passiv (Active/Standby).
- Netztrennung nach Best Practice: Management-, Signalisierungs- und Medien-Netze logisch/physisch trennen.
- Härtung gemäß Best Practice (z. B. CIS/BSI-Empfehlungen).

- Konfigurationsreplikation/Standby-Synchronisation zwischen den RZ-Systemen; PKI-Einbindung für TLS $\geq$ 1.2/mTLS (vgl. Kap. 6.5/7).

2.3 SIP-Trunk & Provider

Der SIP-Trunk wird durch den Auftraggeber bereitgestellt (derzeit Vodafone). Die Vertrags- und Kommunikationsbeziehung mit dem Provider verbleibt vollständig beim Auftraggeber.

Der Auftragnehmer übernimmt im Störfall keine direkte Provider-Koordination, stellt jedoch sämtliche erforderlichen technischen Informationen und Analysen (z. B. SIP-Traces, Log-Dateien, Statusberichte, Fehlerbilder) innerhalb der vereinbarten SLA-Reaktionszeiten bereit. Der Auftragnehmer führt im Rahmen der Fehlerbehebung eine technische Vorqualifizierung durch, identifiziert mögliche SBC-seitige Ursachen und stellt diese dem Auftraggeber strukturiert zur Verfügung. Die Eröffnung und Steuerung von Provider-Tickets erfolgt ausschließlich durch den Auftraggeber. Der Auftraggeber führt die technische Abstimmung mit dem Provider eigenverantwortlich durch und steuert bei Bedarf die Einbindung weiterer Dienstleister. Der Auftragnehmer unterstützt den Auftraggeber bei der Ursachenanalyse durch technische Expertise und stellt alle zur Fehlerdiagnose notwendigen Daten zeitnah bereit.

Der SBC muss die technische Anbindung an die bestehende ttCall-Integration des Auftraggebers unterstützen. Der Auftragnehmer stellt sicher, dass alle für die Anbindung erforderlichen SIP-/Schnittstellenparameter, Header-Durchleitungen (inkl. Reason/Q.850), Protokollmechanismen und Routing-Regeln bereitgestellt und implementiert werden. Die Interoperabilität mit C3000, SIP/TFE und 0800-Transit wird im Rahmen der Abnahme gemäß Kap. 9 nachgewiesen.

Die erfolgreiche Integration mit ttCall ist Voraussetzung für den Go-Live und wird im Rahmen der technischen Abnahme überprüft. Der produktive Regelbetrieb beginnt zu dem im Projektplan bzw. Vergabekalender festgelegten Termin. Weitere Einzelheiten zu Go-Live-Pflichten und Abnahme-Gates siehe Kap. 9.

2.4 Schnittstellen / Abhängigkeiten

Richtung C3000:

- SIP-TLS/mTLS; T.38 (bevorzugt), G.711 A-Law (Fallback) für Faxpfade; weitere Codecs (z. B. G.729) nur nach Bedarf.

Richtung Sonderendpunkte/TFE:

- SIP-TLS/mTLS (sofern verfügbar) bzw. kompatibler SIP-Betrieb mit TLS (mindestens Version 1.2); DTMF nach RFC 2833, inbound und outbound; SIP INFO zulässig; geeignete Codec-Profilen.

0800-Rufnummern:

- reiner Transit (Weiterleitung) an externen Carrier/Dienstleister; keine Wartefeld-/Ansage-/Queue-Logik im SBC; bei Zieltrunk-Down → 503 upstream.

ttCall (Outbound Call Center Lösung des Hersteller ttUnited):

- Sicherstellen der funktionsfähigen Anbindung gemäß Kap. 9 inkl. Header-Pass-Through (From/To/Contact/PAI/PPI/RPID/Diversion/History-Info), Reason/Q.850-Transparenz, Routing-Regeln und Probe-Calls inkl. Medienpfad.

3. Technische Anforderungen und Systemarchitektur

Die in Abschnitt 3.2 definierten SOLL-Anforderungen sind nicht verpflichtend umzusetzen, fließen jedoch mit ihrer Qualität und Vollständigkeit in die Bewertungsmatrix ein. Eine separate Bepreisung der SOLL-Anforderungen erfolgt nicht, ausgenommen hiervon sind ausdrücklich in Kapitel 11 benannte optionale Leistungen, die im Preisblatt zu bepreisen sind.

Der Auftraggeber bewertet den funktionalen Erfüllungsgrad jeweils qualitativ (0–5 Punkte). MUSS-Anforderungen sind vollständig zu erfüllen; SOLL-Anforderungen erhöhen die qualitative Bewertung des Angebots, ohne verpflichtende Umsetzung für den Auftragnehmer.

3.1 MUSS-Anforderungen (funktional/architektonisch)

Der Auftragnehmer hat folgende Anforderungen verbindlich zu erfüllen:

- **Software-SBC:**
Bereitstellung eines Software-SBC, der ohne Virtualisierung direkt auf Windows Server 2025 (Bare Metal) installierbar und betreibbar ist.
- **Redundanz:**
Bereitstellung einer Aktiv/Passiv-Redundanz über zwei Rechenzentrumsstandorte mit einem automatischen Failover von ≤ 5 Minuten. Die manuelle Failover-Prozedur ist vom Auftragnehmer in einer Betriebsdokumentation nachvollziehbar zu beschreiben.
- **Kapazität:**
Der SBC muss mindestens 300 parallele Sessions verarbeiten können. Der Betrieb ist auch im Failover-Szenario (Volllast) sicherzustellen. Der Auftragnehmer berücksichtigt eine Wachstums- bzw. Burstreserve von mindestens +20 %.

- **Sichere Signalisierung und Medien:**
Unterstützung von SIP-TLS (mindestens Version 1.2) sowie mTLS, soweit technisch möglich. SRTP wird verwendet, soweit dies technisch unterstützt oder erforderlich ist. SIP-Signalisierung erfolgt standardmäßig über Port 5061 (TLS) und fällt bei Bedarf auf Port 5060 (TCP) zurück. RTP/SRTP wird über dynamisch ausgehandelte UDP-Ports gemäß geltenden RFC-Standards übertragen.
- **Interoperabilität:**
Der SBC integriert sich vollumfänglich in die Systemlandschaft des Auftraggebers und unterstützt die Anbindung an C3000-Systeme (T.38/G.711), SIP-Sonderendpunkte/TFE sowie SIP-Trunks gemäß Carrieranforderungen (inkl. Early Media, 100rel/PRACK, Diversion/PAI, Reason/Q.850). DTMF wird gemäß RFC 2833 inbound/outbound sowie per SIP INFO unterstützt.
- **ttCall-Integration:**
Der SBC muss die technische Anbindung an die bestehende ttCall-Integration des Auftraggebers unterstützen. Der Auftragnehmer stellt sicher, dass sämtliche für die Integration erforderlichen SIP- bzw. Schnittstellenparameter, Header-Durchleitungen (einschließlich, aber nicht beschränkt auf From/To/Contact/PAI/PPI/RPID/Diversion/History-Info), Protokollmechanismen sowie Routing- oder Signalisierungsregeln bereitgestellt und implementiert werden. Die erfolgreiche Anbindung an ttCall ist Voraussetzung für den Go-Live und wird im Rahmen der technischen Abnahme überprüft. Der produktive Regelbetrieb startet zu dem im Projektplan bzw. Vergabekalender festgelegten Termin. Die Integrationsfähigkeit ist durch den Auftragnehmer nachzuweisen; aus der Anforderung ergeben sich keine Hersteller- oder Produktpräferenzen.
- **Notruf (112/110) und ELIN-Konzept:**
Der Auftragnehmer stellt sicher, dass Notrufe für alle SIP-Nebenstellen (ausgenommen Fax) gemäß ELIN-Konzept abgewickelt werden. Der SBC erkennt Notrufe, ordnet diese anhand hinterlegter Standortinformationen einer standortbezogenen ELIN-Rufnummer zu und signalisiert diese als PAI/CLI an die zuständige Leitstelle (PSAP).
Notrufe haben stets Priorität und umgehen sämtliche Restriktionen (kein CLIR, keine Barring-Listen).
- **Voraussetzung für die ELIN-Funktionalität:**
Da ELIN-Rufnummern aus den vorzuhaltenden Rufnummernblöcken des Auftraggebers gebildet werden, bleibt der Auftraggeber auch im Falle einer

Portierung zu einem externen Provider (OKP) Inhaber dieser Rufnummernblöcke.
Die Nutzung provider-eigener Nummernblöcke für ELIN ist ausgeschlossen.

- **0800-Transit:**

Der SBC leitet 0800-Rufe 1:1 an den externen Carrier/Dienstleister weiter. Header (From/To/Contact/PAI/PPI/RPID/Diversion/History-Info) sind unverändert zu übermitteln. Bei Nicht-Erreichbarkeit des Zieltrunks ist ein SIP-Fehlercode 503 auszugeben.

- **Nummernplan/Normalisierung:**

Umsetzung der E.164-Normalisierung (Inbound/Outbound); administrierbare Blacklist für Ländervorwahlen/Zielmuster; Notrufe bleiben davon unberührt.

Für die Rufnummernrestriktion wird ein COR-Modell (Class of Restriction) mit den Stufen COR 1–9 unterstützt. Die Zuordnung der Rufnummernbereiche erfolgt ausschließlich in einer gesonderten Anlage (15.1.6 COR-Matrix).

- **Administration und Sicherheit:**

Bereitstellung einer GUI-basierten Administration mit RBAC, MFA, Vier-Augen-Prinzip, Topology Hiding, Schutz vor DoS-Grundlast, Peer-Whitelists und definierter Cipher-Policy.

- **Zugangs- und Einsichtsrechte des Auftraggebers:**

Der Auftraggeber erhält unbefristete, personenbezogene und autonome Read-Only-Zugänge (RBAC, MFA, Audit) zum produktiven SBC für Review- und Fehleranalyse Zwecke. Die Einsicht umfasst Status/Alarmer, Routing-/Signalisierungs- und Medienmetriken, Protokolle sowie den Export von Log-/Trace-Daten und nutzungsbezogener und technischer Reports. Nicht-invasive Diagnosen (z. B. SIP-Tracing gemäß Herstellerfunktionalität ohne Serviceunterbrechung) dürfen durch den Auftraggeber eigenständig gestartet werden; konfigurationsändernde Eingriffe erfolgen ausschließlich über das Change-Verfahren gemäß Kap. 12. Abnahmehinweis: Read-Only-RBAC/MFA gem. Kap. 9.

- **Zertifikats- und PKI-Management:**

mTLS-Zertifikatskette; Erneuerungen ≥ 14 Tage vor Ablauf; Alarmierung bei Unterschreitung; Drift-Alarm ≤ 15 Minuten.

- **Monitoring/Integration:**

Unterstützung von SNMPv3 (Polling/Traps), Syslog (Severity-Mapping), Event-Push via REST/Webhook (JSON) oder SMTP; synthetische Probe-Calls inkl. Medienpfad; verschlüsselte Übertragung (TLS ≥ 1.2 /mTLS); MIB/OIDs und Formate werden dokumentiert; Provider-Störungen im Reporting (6.7) separat ausweisen. Abnahmehinweis: Probe-Calls inkl. Medienpfad und Ereigniszustellung gem.

Kap. 9/6.7

- **Backup/Restore:**
Regelmäßige Konfigurations- und Zertifikatsbackups; jährlicher dokumentierter Restore-Test.
- **Hardware:**
- Endgeräte der Firma Avaya (im speziellen die J179) müssen angebunden werden können.

3.2 SOLL-Anforderungen (empfohlen)

Die folgenden Anforderungen sind nicht verpflichtend, werden jedoch im Rahmen der Bewertung berücksichtigt (§ Bewertungsmatrix):

- **API/Automatisierung:**
Bereitstellung geeigneter Schnittstellen (z. B. REST, PowerShell) zur automatisierten Konfiguration und zum Betriebsmanagement.
- **Transcoding/Media-Optimierung:**
Unterstützung bedarfsabhängiger Transcoding- und Media-Optimierungsfunktionen, insbesondere für Audio- und Fax-Pfade.
- **DNS-SRV-Zielauflösung:**
Unterstützung der DNS-SRV-basierten Redundanzauflösung für 0800-Zieltrunks sowie optionaler Alternate-Routing-Strategien.
- **Mandanten-/Mehrinstanzfähigkeit:**
Unterstützung mandanten- oder mehrinstanzfähiger Betriebsmodelle zur Abdeckung zukünftiger Anforderungen.
- **Break-Glass (Step-in, nur Notfall):**
 - Optionaler administrativer Notfallzugang mit Verwaltung im PAM/Vault (MFA, Split-Knowledge/Vier-Augen), vollständiger Auditierung und sofortiger Secret-Rotation nach Nutzung; zulässige Trigger z. B. Nichterreichbarkeit AN > 24/48 Std., Leistungseinstellung/Insolvenz, Sicherheitsvorfall (Sperrung der AN-Konten). Aufbewahrung der Audit-Logs ≥ 12 Monate. Oder gleichwertig.
- **Microsoft Teams Direct Routing – Zertifizierung:**
Der angebotene SBC ist zum Zeitpunkt der Angebotsabgabe als Microsoft Teams Direct-Routing-SBC zertifiziert. Dies dient ausschließlich dem Nachweis der Interoperabilität; eine Nutzung von Teams Direct Routing ist nicht Bestandteil des Leistungsumfangs.

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.

- Lizenzbeschaffung des SBC inkl. erforderlicher Module/Komponenten; Hersteller-Wartung/Supportanspruch.
- Installation & Grundhärtung (Bare-Metal Windows 2025), PKI/mTLS-Einrichtung, Basiskonfiguration.
- Integration: C3000-Schnittstelle (T.38/G.711, TLS/mTLS), Sonderendpunkte/TFE (DTMF-Profil, TLS soweit möglich), SIP-Trunk (Providerprofil, Early Media/100rel/PRACK), 0800-Transit (Zieltrunk, 1:1-Headerweitergabe).
- Dokumentation (deutsch/englisch): As-Built (Topologie, Trunks, Routen, Manipulationsregeln, Zertifikate, Cipher-Policy, HA-Design), Betriebshandbuch/Runbooks (Failover/Failback, Zertifikatswechsel, Notruf/ELIN-Pflegeprozess, Notfallprozeduren), Monitoring-/Backup-Konzepte.
- Konzeptunterlagen (lieferverpflichtend):
- Interoperabilitäts-/Schnittstellenkonzept SBC ↔ C3000 (SIP-Profil, TLS/mTLS-Parameter, T.38/G.711-Fallback, Header-Pass-through, Testfälle)
- Betriebskonzept (Rollen/RACI AG–AN–Provider, Kooperations-SLA/Erstreaktion, Wartungsfenster-Prozess, Störungs-Triage)
- Sicherheitskonzept gemäß Kap. 7.3 / Anlage 15.2.3 sowie Zugriffskonzept gemäß Kap. 7.8 / Anlage 15.2.4 (RBAC/MFA, Admin-Audit, optional: Break-Glass/Step-in inkl. PAM/Vault, Secret-Rotation – sofern vereinbart)
- Test-/Abnahmekonzept (Ableitung Kap. 9 inkl. Evidenzen/Protokollierung)
- DR-/Wiederanlaufkonzept (Failover/Failback, Wiederherstellungskette, Kommunikations-/Escalation-Plan). (Terminisierung und Freigaben gemäß Kap. 13.)
- Know-how-Transfer/Handover an den Betrieb (AG): Admin-/Betriebsworkshop.
- Abnahme nach Testkatalog (siehe Kap. 9).
- Credentials & Konfig-Escrow: Initiale Übergabe aller Zugangsdaten, Lizenz-/Aktivierungs-Informationen, Konfigurations-/Zertifikats-Backups sowie Hersteller-Portalzugänge an den Auftraggeber (Vault/Escrow), inkl. Verfahren zur laufenden Aktualisierung.

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 laufende Betriebsdokumentation. Einmalige Projektleistungen sind in Kapitel 4 beschrieben.

5.2 Betrieb und Monitoring

Der Auftragnehmer stellt den durchgehenden Betrieb des SBC-Systems sicher. Dies umfasst insbesondere ein 24×7-Monitoring aller relevanten Betriebsparameter (u. a. Signalisierung, Registrierungen, Trunk-Status, Zertifikate, Ressourcenverbrauch sowie HA-Status).

Der Service beinhaltet die laufende Überwachung und Pflege des Systembetriebs, einschließlich Kapazitätsmanagement sowie Dokumentationspflege (lebendes Betriebshandbuch).

Zusätzlich betriebene Software- oder Analyse-Tools (z. B. SIP-Analyzer), die auf demselben Server bzw. in einer HA-Serverumgebung installiert sind, unterliegen denselben Betriebs-, Sicherheits-, Monitoring- und Patch-Vorgaben wie der SBC selbst. Der Einsatz dieser Tools darf die SBC-Funktionalität nicht beeinträchtigen und muss vollständig im Managed-Service-Umfang berücksichtigt und dokumentiert sein.

Die Provider-Koordination (Eröffnung/Eskalation von Tickets) erfolgt ausschließlich durch den Auftraggeber. Der Auftragnehmer leistet technische Vorqualifizierung und Zuarbeit (u. a. SIP-Traces, Log-Daten, Ursachen-/Zeitzuordnung Provider vs. SBC, Teilnahme an Troubleshooting Meetings) innerhalb der vereinbarten SLA-Reaktionszeiten. Für Review-/Fehleranalysezwecke steht dem Auftraggeber ein 24×7-Einsichtsrecht auf den SBC gemäß Kap. 3.1 (RBAC/MFA, Audit) zu; der Zugriff ist autonom und bedarf keiner vorherigen Freigabe durch den Auftragnehmer.

Der Auftraggeber behält sich vor den SBC zusätzlich in eigene Monitoringsystem einzubinden. Das entbindet den Auftragnehmer nicht von der Pflicht eines proaktiven Monitorings.

Erreichbarkeit, Ansprechpartner und Betriebsteam (AN):

- **Kontaktkanäle & Störungsannahme:**

Der Auftragnehmer stellt für den produktiven Betrieb eine durchgängig erreichbare Kontaktstruktur bereit: Funktions-E-Mail-Adresse, Ticket-Systemzugang (URL/API) sowie eine telefonische Störungshotline.

Die Störungsannahme ist 24×7, 365 Tage/Jahr möglich; die Bearbeitung erfolgt gemäß Servicezeiten Kap. 6.2 und Priorisierung Kap. 6.1.

Die jeweiligen Kontaktdaten (E-Mail, Hotline, Ticket-URL) werden spätestens zur Inbetriebnahme schriftlich verbindlich benannt und bei Änderungen unverzüglich in schriftlicher Form aktualisiert.

- **Feste Ansprechpartner (Named Contacts):**

Der Auftragnehmer benennt und pflegt feste Ansprechrollen mit Vertretung: Service Manager (operativ/kommerziell) und Technical Lead (technisch), jeweils mit Stellvertretung und klaren Eskalationspfaden (2nd/3rd-Level, Management-Eskalation). Änderungen der Besetzung werden dem Auftraggeber unverzüglich, aber mindestens mit 3 Werktagen Vorlauf, in Textform mitgeteilt.

- **Festes Betriebsteam:**

Der Auftragnehmer stellt ein eingearbeitetes, fest zugeordnetes Betriebsteam für den SBC-Service sicher (2nd/3rd-Level), inkl. Vertretungsregelung, Wissenssicherung (Runbooks, Known-Error-DB) und Onboarding-Prozess für neue Teammitglieder. Übergaben an wechselnde Ad-hoc-Teams sind zu vermeiden.

- **Sprache:**

Der Support wird in deutscher Sprache erbracht; englischsprachige Kommunikation ist auf Wunsch zusätzlich möglich. Ticket-Titel und -Zusammenfassungen werden in Deutsch geführt; technische Anhänge/Logs können englisch sein.

5.3 Wartung und Lifecycle Management

Der Auftragnehmer stellt die Wartung und den vollständigen Lifecycle-Betrieb des SBC-Systems gemäß ITIL-Prozessen sicher (Incident, Problem, Change, Release).

Dies beinhaltet Patch- und Release-Management für die SBC-Software sowie das zugrunde liegende Betriebssystem, einschließlich abgestimmter Wartungsfenster.

Weiter umfasst der Managed Service ein durchgängiges Vulnerabilitäts-Management (Bewertung, Remediation), Konfigurations-Versionierung, Zertifikatsmanagement sowie ein gesichertes Backup-/Restore-Konzept.

Ein vollständiger Wiederherstellungstest (Restore-Test) ist mindestens einmal jährlich durchzuführen und zu dokumentieren.

6. Service Level Agreement (SLA)

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 — auch im Interimbetrieb bis zur vollständigen Abnahme.

6.1 Priorisierungsklassen P1/P2/P3

Die Priorisierung erfolgt anhand der betrieblichen Kritikalität des SBC-Dienstes und wird in drei Stufen (P1–P3) klassifiziert. Die Einstufung orientiert sich an branchenüblichen Priorisierungsmodellen für Echtzeit-Kommunikationssysteme.

P1 – Kritisch:

Schwerwiegende Störung mit unmittelbarer Auswirkung auf den produktiven Kommunikationsbetrieb. Der SBC-Dienst ist vollständig ausgefallen oder erheblich beeinträchtigt. Beispiele:

- vollständiger Ausfall des Session Border Controller (SBC)
- keine oder fehlerhafte Registrierungen für große Nutzergruppen
- Notrufe nicht möglich oder fehlerhaft
- flächendeckende Signalisierungs- oder Audio-Probleme (z. B. einseitiges Audio auf Systemebene)
- Die geschäftliche Kommunikation ist massiv eingeschränkt oder nicht möglich.

P2 – Hoch:

Teilfunktionseinschränkung des SBC-Dienstes mit spürbarer, aber nicht kritischer Beeinträchtigung des Betriebs. Beispiele:

- Störungen bei einzelnen Endpunkten oder Teilsegmenten
- sporadische Fehler bei eingehenden/ausgehenden Anrufen
- eingeschränkte Medienpfade oder Codec-Probleme
- fehlerhafte Funktion einzelner Teilmodule, aber Grundbetrieb weiterhin gegeben
- Der geschäftliche Betrieb ist möglich, jedoch beeinträchtigt.

P3 – Normal:

Nicht-kritische Störung oder Anfrage ohne unmittelbare Auswirkungen auf den operativen Betrieb. Beispiele:

- Anfragen zu Konfigurationsanpassungen (z. B. Routing-Optimierung, Normalisierungsregeln)
- Dokumentations- oder Logging-Themen
- Fragen zur Erweiterung oder Optimierung
- geringfügige Anzeige- oder Komfortfunktionen
- Der produktive Betrieb ist nicht beeinträchtigt.

6.2 Servicezeiten

Die Servicezeiten definieren die Zeitfenster, in denen der Auftragnehmer für Analyse, technische Vorqualifizierung und SLA-Reaktionszeiten zur Verfügung steht (eine Störungsannahme ist 24×7/365 möglich):

- P1: Mo-So, 00:00–23:59 Uhr
- P2: Mo–Fr, 07:00–18:00 Uhr (niedersächsische Feiertage ausgenommen)
- P3: Mo–Fr, 07:00–18:00 Uhr (niedersächsische Feiertage ausgenommen)

Während der Servicezeiten führt der Auftragnehmer die technische Vorqualifizierung gemäß der definierten Priorisierung durch; die Provider-Koordination erfolgt ausschließlich durch den Auftraggeber.

6.3 Reaktions- und Entstörzeiten

Reaktionszeit = Zeitspanne ab Störungsannahme (Zeitstempel des Eingangs der Störungsmeldung in einem vereinbarten Kanal – Ticket/Hotline/Funktionsmail –, 24×7/365) bis zur qualifizierten Rückmeldung; Bearbeitung gemäß Servicezeiten Kap. 6.2.

Qualifizierte Rückmeldung = Eingangsbestätigung mit Ticket-ID, Priorisierung (P1–P3) und erstem Maßnahmenplan/ETA oder Eskalationshinweis.

P1:

- Reaktion: ≤ 15 Minuten
- Bereitstellung eines Workarounds: ≤ 1 Stunde
- Wiederherstellung: ≤ 2 Stunden (sofern innerhalb des Verantwortungsbereichs des Auftragnehmers)

P2:

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

P3:

- Reaktion: ≤ 2 Stunden
- Wiederherstellung: ≤ 8 Stunden (oder Umsetzung im nächsten regulären Wartungsfenster)

Hinweis: Die SLA-Reaktions- und Entstörzeiten gelten ausschließlich für die durch den Auftragnehmer zu erbringenden Tätigkeiten (technische Vorqualifizierung, Analyse und Bereitstellung technischer Daten).

Liegt die Störungsursache außerhalb des SBC (z. B. beim SIP-Trunk-Provider), unterstützt der Auftragnehmer durch technische Zuarbeit; die Ticket-Eröffnung, Eskalation und Koordination mit dem Provider erfolgt ausschließlich durch den Auftraggeber.

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

6.4 Verfügbarkeit & Messung

Monatliche Mindestverfügbarkeit SBC: **≥ 99,9 % (24×7)**

- Verfügbarkeitsformel
$$\text{Verfügbarkeit [\%]} = ((\text{Gesamtzeit} - \text{Ausfallzeit}) / \text{Gesamtzeit}) \times 100$$

(Messzeitraum: Kalendermonat; Zeitbasis: MEZ/MESZ.)
- Messpunkte (informativ, zur Plausibilisierung):
Signalisierungs-Health, Trunk-Status, Registrierungen, synthetische Probe-Calls inkl. Medienpfad.
- Ausnahmen (werden nicht als Ausfallzeit gezählt):
geplante Wartungen gem. Kap. 8.4 (fristgerecht angekündigt), vom AG veranlasste Änderungen/Tests, höhere Gewalt, Provider-Störungen (separat auszuweisen).
- Transparenz: Provider-bedingte Ereignisse und eingeplante Wartungsfenster werden im SLA-Reporting (Kap. 6.7) separat dargestellt.

6.5 Sicherheits-/Zertifikats-/Compliance-KPIs

- TLS ≥ 1.2, mTLS verpflichtend
- SRTP soweit technisch unterstützt
- Zertifikatsverlängerung ≥ 14 Tage vor Ablauf
- Alarmierung bei Unterschreitung der Restlaufzeit
- Konfigurationsdrift-Alarm ≤ 15 Min.
- Admin-Audit-Logs ≥ 12 Monate.

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) beträgt maximal 15 % des monatlichen Serviceentgelts.

6.6.6 Beispiele (ohne Fax-Komponente)

- **Beispiel 1 – Verfügbarkeit unterschritten**

Monatsverfügbarkeit: 99,2 % → Staffel gemäß 6.6.2: 10 % Minderungsbetrag.

- **Fiktives Monatsentgelt: 20.000 €**

- Berechnung:

- $20.000 \text{ €} \times 10 \% = \mathbf{2.000 \text{ € Minderungsbetrag}}$

- Auszahlbares Monatsentgelt:

$$20.000 \text{ €} - 2.000 \text{ €} = \mathbf{18.000 \text{ €}}$$

- **Beispiel 2 – P1-SLA-Verstoß (Wiederherstellungszeit)**

SLA-Ziel: Wiederherstellung ≤ 2 Std.; tatsächlich 5 Std. → 3 begonnene Stunden über Zielzeit.

- Regel gemäß 6.6.3 a): 1 % je begonnener Stunde, max. 5 % → 3 % Minderungsbetrag.

- **Fiktives Monatsentgelt: 20.000 €**

- Berechnung:

- $20.000 \text{ €} \times 3 \% = \mathbf{600 \text{ € Minderungsbetrag}}$

- Auszahlbares Monatsentgelt:

- $20.000 \text{ €} - 600 \text{ €} = \mathbf{19.400 \text{ €}}$

Beispiel 3 – Reportingverstoß

Monats-SLA-Bericht verspätet (vgl. 6.6.4) → 1 % Minderungsbetrag.

- **Fiktives Monatsentgelt: 20.000 €**

- Berechnung:

- $20.000 \text{ €} \times 1 \% = \mathbf{200 \text{ € Minderungsbetrag}}$

- Auszahlbares Monatsentgelt:

- $20.000 \text{ €} - 200 \text{ €} = \mathbf{19.800 \text{ €}}$

- **Gesamtbeispiel (Kumulierung mit Deckelung)**

Verfügbarkeit 10 % + P1-SLA-Verstoß 3 % + Reporting 1 % = 14 % Gesamtsumme.

- **Fiktives Monatsentgelt:** 20.000 €
- Berechnung:
- $20.000 \text{ €} \times 14 \% = \mathbf{2.800 \text{ € Minderungsbetrag}}$
- Auszahlbares Monatsentgelt:
- $20.000 \text{ €} - 2.800 \text{ €} = \mathbf{17.200 \text{ €}}$
- Da die Gesamtsumme von 14 % unterhalb der Deckelung gemäß 6.6.5 liegt, erfolgt keine weitere Begrenzung.
- **Hinweis:** Additive Berücksichtigung mehrerer Auslöser erfolgt stets unter Beachtung der monatlichen Deckelung von 15 % gemäß Ziffer 6.6.5.

6.7 Reporting

6.7.1 Monats-SLA-Report (Pflichtinhalt)

Der Auftragnehmer liefert monatlich einen SLA-Report, der mindestens Folgendes umfasst:

- Verfügbarkeit des SBC-Dienstes (Messzeitraum Kalendermonat)
 - Wert (in %) inkl. Messgrundlage und Ausnahmen gemäß 6.4
 - Zeitliche Darstellung (Tages-/Wochen-Sicht mit Ereignismarkern)
- Incidents & Priorisierung
 - Anzahl und Liste P1/P2/P3, inkl. Start/Ende, Ausfallzeiten (falls relevant), betroffene Funktionen/Trunks
- Root-Cause-Analysen (RCA) für P1/P2
 - Kurz-RCA (technische Ursache, Abhilfemaßnahmen)
 - Erfüllung der Frist gemäß 6.6.4 (RCA innerhalb 1 AT); bei Verzug: Kennzeichnung
- Kapazität & Performance
 - Session-Spitzen/-Durchschnitt, Reserven, Trends
 - Medien-KPI (informativ) inkl. Ergebnis der synthetischen Probe-Calls (Signalisierung + Medienpfad)
- Zertifikats-/Compliance-Status
 - Zertifikate mit Restlaufzeiten (Schwellen: 30/14 Tage), Alarmierungen
 - Drift-Alarme ($\leq 15 \text{ Min}$) und Admin-Audit-Log-Status ($\geq 12 \text{ Monate}$)
- Ereignisübersichten (Transparenzpflichten)
 - Provider-Störungen: separate Ausweisung (Zeit, Ursache/Carrier-Ticket, betroffene Dienste)
 - Geplante Wartungsfenster gemäß 8.4: separate Ausweisung (Termin, Umfang, Impact)
- Service-Credits (Monat)
 - Auslöser gemäß 6.6.1 (Verfügbarkeit, P-basierte SLA-Verstöße, Reporting)

- Berechnung je Auslöser (Staffel/Regel gemäß 6.6.2–6.6.4), Zwischensumme, Deckelprüfung 6.6.5
- Endsumme der Credits (monatlicher Abzug vom Serviceentgelt)
- SOLL (optional): Break-Glass-Ereignisse (Anzahl/Datum/Zweck) inkl. Hinweis auf Audit-Nachweis und Rotationsbestätigung separat ausweisen.

Form: PDF (menschlesbar) und CSV/Excel (Datenexport der Kennzahlen).

Frist: Lieferung bis 5. Arbeitstag des Folgemonats, sofern nichts Abweichendes vereinbart ist.

6.7.2 Quartalsbericht (Analyse & Forecast)

Der Auftragnehmer liefert quartalsweise eine konsolidierte Betrachtung:

- Trendanalysen (Verfügbarkeit, Incidents, P1/P2-Ursachen, Kapazität, Medien-KPI)
- Security-Bewertung (Zertifikats-Lebenszyklen, Drift-/Audit-Lage, relevante Patches)
- Optimierungsvorschläge & Maßnahmenplan (Prioritäten, Aufwand, Nutzen)
- Forecast (Kapazität/Skalierung, Plan für Zertifikatswechsel, potenzielle Wartungsfenster)

Form: Präsentationsformat (PDF/PowerPoint) + Anhang mit Datenbasis.

Termin: innerhalb von 10 Arbeitstagen nach Quartalsende (Q1/Q2/Q3/Q4).

6.7.3 Datenquellen & Nachvollziehbarkeit

- Messbasis: Monitoring-System(e) des Auftragnehmers; Messregeln gemäß 6.4.
- Korrelation: Ereignisse (Incidents, Wartungsfenster, Provider-Störungen) werden zeitlich korreliert dargestellt.
- Belege: Auf Anforderung werden Ausschnitte aus Logs/Traces (zweckgebunden, datenschutzkonform) bereitgestellt, sofern erforderlich, um Kennzahlen/RCA's zu verifizieren.

6.7.4 Abnahme & Nachlieferung

- Abnahme: Der monatliche Report gilt als geliefert, wenn die Frist (siehe 6.7.1) eingehalten und die Pflichtinhalte vollständig sind.
- Nachlieferung: Fehlende/fehlerhafte Inhalte sind innerhalb von 2 AT nach Anzeige nachzuliefern/zu korrigieren.
- Konsequenz bei Pflichtverletzung: Credits gemäß 6.6.4 (Reporting-Verstoß) bleiben unberührt.

6.7.5 Änderungen am Reporting

- Inhaltliche/formatielle Änderungen (z. B. zusätzliche KPIs, neues Layout) erfolgen in Abstimmung mit dem Auftraggeber und werden im Betriebshandbuch (Reporting-Kapitel) schriftlich dokumentiert.
- Automatisierungs-/Schnittstellenwünsche (z. B. Ticket-API, Daten-Feeds) können im Rahmen des Change-Verfahrens (Kap. 12) umgesetzt werden.

6.8 Service-Credits, Messung und Verantwortungsgrenzen

Service-Credits sind pauschalierte 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 SBC-Dienst relevanten Datenschutz-, Informationssicherheits- und Betriebsanforderungen widerspruchsfrei in den jeweils geschuldeten Konzepten umzusetzen. Die Konzepte sind aufeinander abzustimmen und während der Vertragslaufzeit aktuell zu halten.

Der SBC-Dienst verarbeitet insbesondere Kommunikationsmetadaten, Signalisierungsdaten, technische Betriebsdaten, Administrationsdaten, Protokolle, Reports, SIP-Traces und Diagnoseinformationen. Soweit im Einzelfall personenbezogene Daten oder Sozialdaten betroffen sein können, sind diese zweckgebunden, datensparsam und zugriffsbeschränkt zu verarbeiten.

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 personenbezogene 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.

Nicht erforderliche Datenverarbeitungen, Protokollierungen, Exporte oder Einsichtsmöglichkeiten sind zu vermeiden oder auf das erforderliche Maß zu begrenzen. Soweit technisch möglich und fachlich ausreichend, sind Daten zu pseudonymisieren, zu anonymisieren oder aggregiert bereitzustellen.

7.3 Sicherheitskonzept

Der Auftragnehmer erstellt ein eigenständiges, systembezogenes Sicherheitskonzept für den bereitgestellten SBC-Dienst.

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 Management-, Signalisierungs- und Medienpfaden,
- 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

Der Auftragnehmer setzt für alle im Rahmen dieses Loses eingesetzten Systeme eine angemessene System- und Betriebssystemhärtung nach anerkanntem Stand der Technik um. Als Orientierung können BSI IT-Grundschutz, CIS Benchmarks oder vergleichbare herstellerneutrale Sicherheitsbaselines herangezogen werden, soweit diese auf die eingesetzten Komponenten anwendbar sind.

7.5 BSI-Bezug für VoIP- und TK-Sicherheitsanforderungen

Für VoIP-, SIP-, Signalisierungs-, Medien- und SBC-Komponenten sind die einschlägigen Anforderungen und Empfehlungen des BSI zu berücksichtigen, soweit diese auf den konkreten Dienst und die eingesetzte Kommunikationsarchitektur anwendbar sind. Dies umfasst insbesondere eine Orientierung am IT-Grundschutz-Baustein NET.4.2 VoIP sowie, soweit einschlägig, am BSI-Kompodium für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf (KomTK).

Eine vollständige Umsetzung einzelner BSI-Kompodien 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- und Nachweisdaten mit Personenbezug sind zweckgebunden nur solange vorzuhalten, wie dies für Betrieb, Störungsanalyse, Sicherheitsnachweis, Auditierung 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.

Inhaltsnahe Daten und Detaildaten, insbesondere SIP-Traces, Diagnoseexporte, Paketmitschnitte oder vergleichbare Analysedaten, 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 SBC-Dienst.

Das Zugriffskonzept beschreibt die konkrete Ausgestaltung der Zugriffsmöglichkeiten auf Systeme, Administrationsoberflächen, Schnittstellen, Protokolle, Reports, Monitoringdaten, Konfigurationsdaten und sonstige betriebsrelevante Informationen.

Das Zugriffskonzept umfasst insbesondere:

- Rollen- und Berechtigungsmodelle,
- administrative und privilegierte Zugriffe,
- Rollen nach dem Prinzip der minimal erforderlichen Berechtigungen,
- RBAC,
- Mehr-Faktor-Authentifizierung,
- 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, insbesondere SIP-Tracing,
- Rezertifizierung von Berechtigungen,
- Entzug und Änderung von Berechtigungen,
- Protokollierung und Nachvollziehbarkeit administrativer Zugriffe,
- Umgang mit Service-, Funktions- und Notfallkonten,
- Regelungen zu Break-Glass- bzw. Step-in-Zugängen, soweit vereinbart,
- Abgrenzung zwischen Auftraggeber, Auftragnehmer, Hersteller 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, Kommunikationsmetadaten, SIP-Traces, 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.

Die Provider-Koordination verbleibt beim Auftraggeber, soweit nicht ausdrücklich anders vereinbart; der Auftragnehmer stellt die erforderlichen technischen Informationen und Analysen bereit.

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 die Log- und Protokolldateien sind darzustellen. SIP-Traces und vergleichbare Detaildaten dürfen nur anlassbezogen und zweckgebunden verarbeitet, exportiert und aufbewahrt werden.

8.3 Monitoring

Integration via SNMPv3 und Syslog in Systeme des Auftraggebers (Zielangaben Hostname/IP). Die Überwachung umfasst insbesondere Signalisierungs- und Medienparameter, Registrierungen, Trunk-Status sowie Systemressourcen. Ergänzend gelten die Integrationsanforderungen aus Kap. 3.1 (Event-Push/Probe-Calls).

Media-KPIs (informativ/Thresholds):

Jitter ≤ 30 ms

Packet-Loss ≤ 1 %

One-Way-Latency ≤ 150 ms

8.4 Wartungsfenster & Notfall-Changes

Es werden zwei Arten von Wartungsfenstern definiert:

- **1. Reguläres Wartungsfenster (Low-Impact-Changes):**
Mo–Fr, ab 20:00 - 06:00 Uhr des Folgetages.
Für Änderungen ohne erwartete Dienstunterbrechung (z. B. Routing-Anpassungen, Normalisierungsregeln, Monitoring-Konfigurationen, Zertifikatsimporte ohne Neustart).
Vorlauf: ≥ 20 Arbeitstage.
- **2. Erweitertes Wartungsfenster (High-Impact-Changes):**
Samstag 00:00 – Sonntag 23:59 Uhr.

Alle Low-/High-Impact-Changes sind dem Auftraggeber in Textform anzumelden und zu bestätigen.

Notfall-Changes werden außerhalb der definierten Wartungsfenster unmittelbar durchgeführt, sofern erforderlich. Eine Anmeldung und Freigabe durch den Auftraggeber ist dennoch erforderlich (Textform); Umsetzung nur mit dokumentiertem Risiko- und Rollback-Plan; Nachdokumentation im SLA-Reporting gem. Kap. 6.7.

9. Abnahme

- **Installation/Plattform:**

Bare-Metal-Installation Windows 2025, Härtung, mTLS-Einrichtung, Cipher-Policy.

- **HA/Failover:**

geplanter Failover (RZ-Wechsel) ≤ 5 Min, Failback; Nachweis Probe-Calls/Medienpfad.

- **SIP-Trunk:**

Interop mit Provider (Early Media, 100rel/PRACK, Diversion/PAI), Fehlertransparenz (Reason/Q.850).

- **C3000-Schnittstelle:**

T.38/G.711 (in/out), TLS/mTLS; Reporting enthält T.38/G.711-Auflösung/Retrys.

- **Sonderendpunkte/TFE:**

Registrierung/Calls, DTMF RFC2833/SIP INFO; Codec-Profile.

- **ttCall-Integration:**

erfolgreiche Anbindung gemäß Abschnitt 2.3/3.1 (Header-Durchleitungen, Routing-Regeln, Probe-Calls inkl. Medienpfad); Abnahme vor Go-Live.

- **0800-Transit:**

1:1-Headerweitergabe (From/To/Contact/PAI/PPI/RPID/Diversion/History-Info), Zieltrunk-Down $\rightarrow$ 503 upstream; keine lokale Audio-Behandlung.

- **Notruf (112/110):**

ELIN-Signalisierung gemäß Nebenstellen-Zuordnung; Tests nur koordiniert (oder mit Provider-Testnummern).

- **Monitoring/SIEM:**

SNMPv3/Syslog-Events sichtbar (Trunk-Down, Zertifikat < 14 Tage, HA-Event), Probe-Calls mit Medienpfad.

- **Backup/Restore:**

Vollständiger Restore-Test (Konfig/Zertifikate).

- **Dokumentation:**

As-Built, Betriebshandbuch/Runbooks vollständig.

- **Konzeptunterlagen:**

Interoperabilitäts-/Schnittstellenkonzept SBC ↔ C3000 (SIP-Profil, TLS/mTLS-Parameter, T.38/G.711-Fallback, Header-Pass-through, Testfälle) – vorgelegt, geprüft, freigegeben.

Betriebskonzept (Rollen/RACI AG–AN–Provider, Kooperations-SLA/Erstreaktion, Wartungsfenster-Prozess, Störungs-Triage) – 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-/Abnahmekonzept (Ableitung Kap. 9 inkl. Evidenzen/Protokollierung) – vorgelegt, geprüft, freigegeben.

DR-/Wiederanlaufkonzept (Failover/Failback, Wiederherstellungskette, Kommunikations-/Escalation-Plan) – vorgelegt, geprüft, freigegeben.

Die Terminierung der Konzept-Vorlagen/Freigaben erfolgt gemäß Kap. 13.

- **AG-Zugänge (RBAC/MFA):**

Nachweis der eingerichteten, personenbezogenen Read-Only-Rollen (RBAC) mit MFA; erfolgreicher Login durch AG, Einsicht in Status/Alarmer, Routen/Signalisierungs- und Medienmetriken sowie Export eines SIP-Trace (nicht-invasiv, ohne Serviceunterbrechung); Verifikation der Audit-Log-Aufzeichnung (Kap. 7) und Aufbewahrungskonfiguration (≥ 12 Monate).

- **Credentials & Konfig-Escrow:**

Inventar der übergebenen Credentials/Lizenzen/Hersteller-Zugänge/Backups (inkl. Prüfsummen/Hash-Werte), Nachweis der Hinterlegung im PAM/Vault des AG sowie des Aktualisierungsverfahrens.

- **SOLL (optional) – Break-Glass (Step-in):**

Nachweis eines Dry-Run (Anmeldung, vollständiges Audit-Log, sofortige

Secret-Rotation), inkl. Dokumentation der definierten Trigger (vgl. Kap. 3.2, Kap. 7.8 und Kap. 10). Bewertung gemäß Bewertungsmatrix (Anlage 15.1.3.).

- **Abnahme-Gate (Go-Live):**

Die Freigabe zum Go-Live setzt folgende erfolgreiche Nachweise voraus:

- Infrastrukturelle Integration: HA/Failover ≤ 5 Min inkl. Failback, Monitoring-Anbindung (SNMP/Syslog/REST) und synthetische Probe-Calls inkl. Medienpfad, PKI/Zertifikate, Backup/Restore, RBAC/MFA/Audit.
- C3000-Integration: T.38 (bevorzugt) mit G.711-Fallback, TLS/mTLS, ein-/ausgehende Faxpfade, konsistente Header/Reason/Q.850.
- SIP-Sonderendpunkte/TFE: Registrierung, bidirektionaler Rufaufbau, DTMF nach RFC 2833/SIP INFO, passende Codec-Profile.
- 0800-Transit: 1:1-Headerweitergabe, Zieltrunk-Down $\rightarrow$ 503 upstream, keine lokale Audio-Behandlung.
- ttCall-Integration: Funktionsfähige Anbindung gemäß Abschn. 2.3/3.1.
- AG-Zugänge & Escrow: Read-Only-RBAC/MFA und Credentials/Escrow (Kap. 4/10).
- Der SLA-Start gemäß Kap. 6 erfolgt ab Go-Live; weitergehende Prüfpunkte können per Teilabnahme/Re-Test nachgezogen werden.
- Nichtabnahme/Mängelbeseitigung, Re-Test & Interimsbetrieb
- Werden einzelne Prüfpunkte verfehlt, ist der Auftragnehmer zur Mängelbeseitigung verpflichtet. Der Auftraggeber kann die Abnahme teilweise verweigern und Teilabnahmen auf abgeschlossene Prüfpunkte beschränken. Re-Tests erfolgen innerhalb eines angemessenen, gemeinsam festzulegenden Zeitraums.

Interimsbetrieb und Verantwortlichkeit:

Unabhängig vom Abnahmefortschritt stellt der Auftragnehmer ab Go-Live und bis zum Beginn des produktiven Regelbetriebs sowie bis zur vollständigen Abnahme den durchgehenden Betrieb, die Entstörung und die Sicherheit des SBC im produktiven Umfeld sicher. Ein Verzug bei der Abnahme entbindet den Auftragnehmer nicht von seinen Pflichten.

SLA-Anwendung im Interimsbetrieb:

Für den Interimsbetrieb gelten die Servicezeiten gemäß Kap. 6.2, die Reaktions-/Entstörzeiten gemäß Kap. 6.3 sowie die Sicherheits-/Zertifikats-/Compliance-KPIs gemäß Kap. 6.5. Die Verfügbarkeit gemäß Kap. 6.4 wird ab Go-Live gemessen; Service-Credits gemäß Kap. 6.6 werden ab Go-Live monatlich angewandt.

Mängelklassen und verkürzte Fristen:

Abnahmeverhindernde Mängel (Klasse A) sind insbesondere: ttCall-Integrationsfehler, Notruf/ELIN-Fehlfunktionen, SBC-Gesamtausfälle, HA/Failover-Nichterfüllung, kritische Sicherheitsmängel (z. B. aktiv ausnutzbare Schwachstellen). Klasse A ist innerhalb von 48 Stunden zu beheben oder durch einen wirksamen Workaround zu neutralisieren; dauerhafte Fehlerbehebung innerhalb von 5 Arbeitstagen.

Abnahmehemmende Mängel (Klasse B) beeinträchtigen Funktionen spürbar, verhindern die Abnahme jedoch nicht. Klasse B ist innerhalb von 10 Arbeitstagen zu beheben oder durch einen Workaround zu neutralisieren; dauerhafte Fehlerbehebung innerhalb von 20 Arbeitstagen.

Mängel der Dokumentation (Klasse C) sind innerhalb von 5 Arbeitstagen zu beheben.

Kosten & Ressourcen:

Mängelbeseitigung einschließlich Workarounds, Re-Tests und notwendiger zusätzlicher Ressourcen erfolgt für den Auftraggeber kostenfrei.

Step-in & Break-Glass (keine Haftungsverschiebung):

Übt der Auftraggeber bei Nichterreichbarkeit oder Leistungsverweigerung des Auftragnehmers die Step-in-Rechte gemäß Kap. 3.1/12 aus (Break-Glass), berührt dies nicht die Verantwortlichkeit des Auftragnehmers für den vertragsgemäßen Zustand und die Mängelbeseitigung. Nach Nutzung des Break-Glass-Zugangs erfolgt unverzügliche Secret-Rotation; sämtliche Eingriffe werden lückenlos protokolliert.

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 nur verarbeitet werden, soweit dies für die jeweilige Test- oder Abnahmehandlung erforderlich ist. Vor produktiver Freigabe und außerhalb ausdrücklich freigegebener Betriebs-, Test- oder Abnahmehandlungen erhält der Auftragnehmer keinen Zugriff auf Produktivsysteme oder produktive personenbezogene Daten. Erforderliche produktive Zugriffe im Interims- oder Regelbetrieb erfolgen ausschließlich nach Freigabe des Auftraggebers, zweckgebunden, rollenbasiert und protokolliert.

10. Rollen, Abgrenzung, Mitwirkung

10.1 Auftragnehmer (AN)

- Installation, Betrieb & Betreuung des SBC inkl. Monitoring, Entstörung, technischer Vorqualifizierung und Zuarbeit im Störfall; die Provider-Koordination (Ticket/Eskalation) erfolgt durch den Auftraggeber.
- Administration, Patch und Release Management der SBC-Lösung einschließlich der hierfür durch den Auftraggeber bereitgestellten Windows Server sowie Zertifikats, Schlüssel und Kapazitätsmanagement.
- Pflege Dokumentation, SLA-/Quartalsberichte, Teilnahme an Betriebs-/Security-Jour fixes.
- Interimsbetrieb: Der Auftragnehmer stellt ab Go-Live bis zur vollständigen Abnahme den produktiven Interimsbetrieb gemäß den SLA-Regelungen aus Kap. 6 sicher.
- Credentials & Escrow: Übergabe initialer Admin-Credentials, Lizenz-/Aktivierungsdaten, Konfig-Backups, Zertifikate/Private Keys (soweit AG-eigen) sowie Hersteller-Portalzugänge in versiegelter, vom Auftraggeber verwahrter Form (Vault/Escrow); unverzügliche Aktualisierung bei Änderungen.
- SOLL (optional): Unterstützt die initiale Einrichtung/Tests des Break-Glass-Zugangs (PAM/Vault, MFA, Audit) bei vereinbarter Option.

10.2 Auftraggeber (AG) – Mitwirkung

- 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 inkl. Providerkontakte/SLAs.
- Bereitstellung Zertifizierungsstelle/Trust bzw. Ausstellung von Zertifikaten.
- Bereitstellung ELIN-Verzeichnis (Nebenstelle → Standort → ELIN) sowie Pflegeprozess.
- Freigabe Wartungsfenster, Test-Rufnummern, Ansprechpartner.
- Zugangsverwaltung & PAM: Betrieb des Privileged-Access-Management/Vault; Verwahrung Break-Glass-Zugangsdaten in Split-Knowledge; revisionssichere Protokollierung.
- SOLL (optional): Betreibt das PAM/Vault (Split-Knowledge, Vier-Augen), pflegt die berechtigten Personen und dokumentiert Freigaben schriftlich.

11. Optionen

- Rufbereitschaft außerhalb Regelzeiten (z. B. P2/P3 24×7).
- Erweitertes Monitoring / SIP-Tracing (Langzeitmitschnitte nach Freigabe).
- Change-Kontingente (z. B. 6–8 Std./Monat).
- Skalierung (Erhöhung Session-Lizenzen).
- Alternate-Route/DNS-SRV-Mehrfachziele für 0800-Transit (später aktivierbar).
- Regelstundensatz Techniker, für z.B. Projekte und Weiterentwicklungen
- Regelstundensatz Projektleiter, für z.B. Projekte und Weiterentwicklungen
- Stundensatz Techniker außerhalb Regelzeit, für z.B. Deeskalation und Wiederherstellung (Recovery) oder Verfügbarkeits-/Failover-Management
- Stundensatz Projektleiter außerhalb Regelzeit, für z.B. Deeskalation und Wiederherstellung (Recovery) oder Verfügbarkeits-/Failover-Management

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 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 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.

Restore-Tests und Wiederherstellungsübungen sind regelmäßig, mindestens jährlich, durchzuführen und zu dokumentieren. Dabei ist nachzuweisen, dass die für den Betrieb erforderlichen Konfigurations-, Zertifikats- und Systemdaten innerhalb der vorgesehenen Wiederherstellungsprozesse vollständig und funktionsfähig wiederhergestellt werden können.

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. Hierzu zählen insbesondere Hochverfügbarkeitsarchitektur, Failover- und Fallback-Szenarien, Wiederanlaufreihenfolgen, Kommunikations- und Eskalationswege sowie Nachweise zur Betriebsfähigkeit nach Wiederanlauf.

Das Notfall- und Wiederanlaufkonzept beschreibt insbesondere die 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 IT-Services. 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 Dienstes 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.

Personenbezogene Daten, Protokolle, Reports, Trace-Daten, Diagnoseinformationen 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.

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
- 15.1.6 COR-Matrix

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.