ONELOG
Self-Healing IT Platform

Technisch-organisatorische Maßnahmen (TOMs)

gemäß Art. 32 DS-GVO i.V.m. § 64 BDSG

Auftragsverarbeiter	Pioneerdesk GmbH, Sitz in Deutschland
Plattform	OneLog Enterprise — Self-Healing IT Platform
Dokumentversion	**6.0**
Gültig ab	16.03.2026
Klassifikation	**ÖFFENTLICH / TLP:CLEAR — Freigegeben zur Publikation**
Zielgruppen	KRITIS-Betreiber (Kliniken, Energieversorger), Behörden mit Verschlusssachen (VS-NfD), NATO-Umgebungen, Managed Service Provider (MSP), Banken und Versicherungen (BaFin/VAIT/BAIT)

Rechtsgrundlagen	Art. 32 DS-GVO, § 64 BDSG, Art. 28 Abs. 3 lit. c DS-GVO, § 8a BSI-Gesetz (KRITIS), NIS2-Richtlinie (EU) 2022/2555, BSI TR-02102 (Kryptografie), BaFin VAIT/BAIT/KAIT

Zertifizierungsfundament: ISO/IEC 27001:2022

Die Pioneerdesk GmbH ist seit **Juli 2025** durch die **DICAS GmbH** (akkreditierte Zertifizierungsstelle) nach **ISO/IEC 27001:2022** zertifiziert.

Zertifizierter Scope:
„Planning, development, operation, support of the self-healing IT platform. Detection, analysis, and resolution of IT disruptions in Windows environments."

Sämtliche in diesem Dokument beschriebenen technisch-organisatorischen Maßnahmen sind **integraler Bestandteil des zertifizierten Informationssicherheits-Managementsystems (ISMS)** der Pioneerdesk GmbH. Das ISMS wird kontinuierlich betrieben und unterliegt einem dokumentierten Plan-Do-Check-Act-Zyklus (PDCA) gemäß den Anforderungen der ISO/IEC 27001:2022.

Regelmäßige Überprüfung:

MASSNAHME	ZYKLUS	VERANTWORTLICH
Jährliches Überwachungsaudit (Surveillance Audit)	12 Monate	DICAS GmbH (externe Zertifizierungsstelle)
Re-Zertifizierungsaudit	36 Monate	DICAS GmbH
Internes ISMS-Audit	Halbjährlich	Informationssicherheitsbeauftragter (ISB), Pioneerdesk GmbH
Management-Review	Jährlich	Geschäftsführung, Pioneerdesk GmbH
Risikobewertung (Statement of Applicability)	Anlassbezogen, mindestens jährlich	ISB in Abstimmung mit der Geschäftsführung

Die ISO/IEC 27001:2022-Zertifizierung umfasst die Annex-A-Controls in den Bereichen Informationssicherheitsrichtlinien (A.5), Organisation (A.6), Personalsicherheit (A.7), Vermögenswerte (A.8), Zugangssteuerung (A.9), Kryptografie (A.10), physische Sicherheit (A.11), Betriebssicherheit (A.12), Kommunikationssicherheit (A.13), Systembeschaffung (A.14), Lieferantenbeziehungen (A.15), Störungsmanagement (A.16) und Business Continuity (A.17).

Präambel

Das vorliegende Dokument beschreibt die technisch-organisatorischen Maßnahmen (TOMs) der Pioneerdesk GmbH als Auftragsverarbeiter im Sinne des Art. 28 DS-GVO für die Plattform **OneLog Enterprise**.

Die Maßnahmen gewährleisten den Schutz personenbezogener Daten — einschließlich **besonderer Kategorien gemäß Art. 9 DS-GVO** (Gesundheitsdaten) — unter besonderer Berücksichtigung der erhöhten Schutzanforderungen für:

- **KRITIS-Betreiber** nach § 8a BSI-Gesetz und NIS2-Richtlinie (Kliniken, Energieversorger)
- **Behörden mit Verschlusssachen** (VS-NfD-Anforderungen)
- **NATO-Umgebungen** (STANAG 4774 Datenklassifikation)
- **Finanzsektor** (BaFin VAIT/BAIT/KAIT-Anforderungen)
- **Managed Service Provider** (Multi-Tenant-Isolation, Mandantentrennung)

OneLog Enterprise verarbeitet im Auftrag des Verantwortlichen IT-Infrastrukturdaten, Endgerätedaten (Inventar, Software, Netzwerkstatus) sowie Nutzerdaten (Anmeldeinformationen, Audit-Trails) im Rahmen der automatisierten Störungserkennung, -analyse und -behebung. **Es werden keine Patientendaten, Befunde oder medizinischen Dokumentationen durch die Plattform verarbeitet.** Der Verarbeitungsgegenstand beschränkt sich auf die IT-Betriebsinfrastruktur des Auftraggebers.

1. Vertraulichkeit

1.1 Zutrittskontrolle — Sovereign Cloud Hosting bei STACKIT

Maßnahmen, die Unbefugte am physischen Zutritt zu Datenverarbeitungsanlagen hindern.

Die gesamte Produktivinfrastruktur von OneLog Enterprise wird **ausschließlich** auf der Sovereign Cloud-Plattform **STACKIT** der Schwarz-Gruppe (Schwarz Digital GmbH & Co. KG) betrieben.

MASSNAHME	BESCHREIBUNG
Rechenzentrumsstandort	STACKIT Rechenzentrum EU01 in Heilbronn, Bundesrepublik Deutschland. Eigener europäischer Hyperscaler der Schwarz-Gruppe mit physisch gesicherten Rechenzentren auf deutschem Hoheitsgebiet.

BSI-C5-Testat	STACKIT verfügt über das BSI-C5-Testat (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik. Dies bestätigt die Einhaltung der verschärften Anforderungen an Cloud-Dienstleister für die öffentliche Verwaltung und KRITIS-Betreiber.
Physische Sicherheit	Mehrstufiges Zutrittskontrollsystem mit biometrischer Authentifizierung, Videoüberwachung (24/7/365), Sicherheitsschleusen, Zwei-Personen-Regel (Four-Eyes-Principle) für sicherheitskritische Bereiche sowie permanente Sicherheitsdienstpräsenz.
Datenresidenz	Sämtliche Daten (Data-at-Rest, Backups, Logs, Schlüsselmaterial, KI-Verarbeitungsergebnisse) verbleiben **ausnahmslos** innerhalb der Bundesrepublik Deutschland. Es findet keine Übermittlung in Drittländer statt — auch nicht zu Zwecken der Wartung, des Supports, der Analyse oder der KI-Verarbeitung.

Ausschluss extraterritorialer Zugriffe (Zero CLOUD Act-Risiko):

STACKIT unterliegt als deutsches Unternehmen der Schwarz-Gruppe **keinerlei** extraterritorialer US-amerikanischer Gesetzgebung. Im Einzelnen:

- **CLOUD Act** (Clarifying Lawful Overseas Use of Data Act) — nicht anwendbar
- **FISA Section 702** (Foreign Intelligence Surveillance Act) — nicht anwendbar
- **Executive Order 12333** — nicht anwendbar
- **PATRIOT Act / National Security Letters** — nicht anwendbar

Ein behördlicher Zugriff durch US-amerikanische oder sonstige außereuropäische Stellen auf die im Auftrag des Verantwortlichen verarbeiteten Daten ist **rechtsstrukturell ausgeschlossen**. Dies stellt einen wesentlichen Unterschied zu Cloud-Anbietern mit US-amerikanischer Konzernstruktur dar (AWS, Azure, Google Cloud), bei denen ein solcher Zugriff trotz europäischer Rechenzentrumsstandorte rechtlich nicht ausgeschlossen werden kann.

Relevanz für Zielgruppen:

ZIELGRUPPE	BEDEUTUNG DER SOVEREIGN CLOUD
Kliniken (KRITIS)	Keine Gefahr des Zugriffs auf IT-Betriebsdaten durch US-Behörden. Erfüllung § 8a BSI-Gesetz.
Behörden (VS-NfD)	Ausschließlich deutsche Rechtshoheit. Kein Cloud Act-Risiko. BSI-C5-konform.
NATO-Umgebungen	Europäischer Hyperscaler ohne transatlantische Jurisdiktionskonflikte.

Banken/Versicherungen	BaFin VAIT 4.2 (Informationsrisikomanagement) und BAIT 8.4 (Auslagerung) erfüllt.
MSP	Mandantenisolation auf Sovereign Infrastructure ohne Drittlandtransfer.

Organisatorische Ergänzungen:

- Die Pioneerdesk GmbH unterhält **keine** eigenen physischen Serverräume oder Rechenzentren.
- Administrative Zugänge zur Cloud-Infrastruktur sind ausschließlich über verschlüsselte Kanäle (SSH, VPN) mit vorgeschalteter Multi-Faktor-Authentifizierung möglich.
- Der Kreis der Personen mit Infrastrukturzugang ist auf das erforderliche Minimum beschränkt (Need-to-Know-Prinzip, dokumentiert im ISMS).

1.2 Zugangskontrolle — Authentifizierung und Session-Sicherheit

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

1.2.1 Multi-Faktor-Authentifizierung (MFA/2FA)

VERFAHREN	TECHNISCHE UMSETZUNG
TOTP (Time-Based One-Time Password)	Implementierung gemäß RFC 6238. TOTP-Geheimnisse werden pro Benutzer mit **AES-256-GCM** verschlüsselt gespeichert (Schlüssel im STACKIT Secrets Manager Vault). Zweistufige Validierung: (1) E-Mail + Passwort → temporäres Einmal-Token (5 Minuten TTL, nach einmaliger Verwendung sofort invalidiert), (2) Einmal-Token + TOTP-Code → authentifizierte JWT-Session.
WebAuthn / FIDO2	Vollständige Unterstützung hardwarebasierter Authentifizierung gemäß W3C WebAuthentication Standard. Unterstützte Authentifikatoren: YubiKey, Bitwarden, 1Password, Apple Touch ID, Windows Hello. Erkennung geklonter Sicherheitsschlüssel durch kryptografisches Sign-Counter-Tracking.
MFA-Secret-Verschlüsselung	Alle TOTP-Geheimnisse werden auf Anwendungsebene mit AES-256-GCM verschlüsselt (zufälliger Nonce pro Verschlüsselungsvorgang). Der Verschlüsselungsschlüssel (`MFA_ENCRYPTION_KEY`) wird ausschließlich aus dem STACKIT Secrets Manager geladen. Bestehende Klartext-Secrets werden beim Serverstart automatisch migriert. Format: `$enc$<Base64(Nonce || Ciphertext || Tag)>` .
Erzwingung	MFA kann mandantenspezifisch als obligatorisch konfiguriert werden. Ohne vollständig abgeschlossene MFA-Verifikation wird **keine** authentifizierte Session erstellt.

1.2.2 Passwort-Sicherheit — Argon2id (BSI TR-02102)

Die Plattform setzt **Argon2id** als primären Passwort-Hashing-Algorithmus ein — empfohlen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI TR-02102) und Gewinner des Password Hashing Competition (PHC 2015):

PARAMETER	WERT	BEGRÜNDUNG
Algorithmus	Argon2id	Hybride Variante: Schutz gegen GPU-Angriffe (Argon2i) UND Seitenkanalangriffe (Argon2d). BSI TR-02102-konform.
Speicherbedarf (memory)	64 MB (65.536 KiB)	Jeder Hash-Vorgang belegt 64 MB RAM. GPU/ASIC-Angriffe werden durch den Speicherbedarf wirtschaftlich unrentabel.
Iterationen (time)	1	Optimiert für serverseitiges Hashing bei hoher Parallelität.
Parallelität (threads)	4	Nutzt Multi-Core-CPUs für schnelle Validierung, erhöht GPU-Kosten für Angreifer.
Schlüssellänge	256 Bit (32 Byte)	Äquivalent zu AES-256 Sicherheitsniveau.
Kryptografisches Salz	128 Bit zufällig (`crypto/rand`)	Einzigartig pro Passwort, verhindert Rainbow-Table-Angriffe.
Speicherformat	`$argon2id$v=19$m=65536,t=1,p=4$<Salt>$<Hash>`	Selbstbeschreibend, versioniert, aufwärtskompatibel.

Abwärtskompatibilität: Legacy-Passwörter (Trinity Hash Fusion, bcrypt) werden bei der nächsten Anmeldung transparent auf Argon2id migriert. Es ist keine manuelle Passwortänderung durch Benutzer erforderlich.

SICHERHEITSEIGENSCHAFT	BESCHREIBUNG
Memory-Hardness	64 MB pro Hash macht Brute-Force-Angriffe mit GPUs/ASICs wirtschaftlich unrentabel (Kosten pro Hash: ~1000x höher als bei SHA-256/bcrypt).
Timing-sicherer Vergleich	`crypto/subtle.ConstantTimeCompare()` verhindert Timing-Seitenkanalangriffe.
BSI-Konformität	Argon2id erfüllt die Anforderungen der BSI TR-02102 an Passwort-Hashing-Verfahren.

1.2.3 Session-Management (JSON Web Tokens)

MASSNAHME	UMSETZUNG
Signaturalgorithmus	**Ed25519 (EdDSA)** — moderne elliptische Kurven-Signatur auf Edwards-Kurve. Signaturverifikation erfolgt **vor** der Payload-Dekodierung (Fail-Fast-Prinzip bei Manipulationsversuchen).
Token-Lebensdauer	**15 Minuten** (KRITIS-Härtung, Sprint 9). Ablaufprüfung bei jeder einzelnen API-Anfrage.
Token-Revokation	Sofortige serverseitige Invalidierung über Redis-gestützte Blacklist. Logout zerstört die Session unmittelbar.
Cookie-Sicherheit	Ausschließlich `httpOnly` -Cookies mit `Secure` - und `SameSite=Strict` -Flags — kein Zugriff über JavaScript oder localStorage. Schutz vor XSS-basiertem Token-Diebstahl. Cookie-MaxAge: 900 Sekunden (synchron mit JWT-TTL).
Schlüsselverwaltung	Ed25519-Schlüsselpaar wird aus einem 32-Byte-Seed im STACKIT Secrets Manager rekonstruiert. Kein privater Schlüssel auf dem Dateisystem.

Relevanz für regulierte Umgebungen:

ANFORDERUNG	ERFÜLLUNG DURCH 15-MINUTEN-TTL
BaFin VAIT 4.3	Zeitliche Begrenzung authentifizierter Sessions. Minimales Zeitfenster bei Token-Kompromittierung.
BSI-Grundschutz SYS.1.1.A6	Automatische Session-Terminierung nach definierter Inaktivitätszeit.

KRITIS § 8a	Reduzierte Angriffsfläche durch kurze Token-Lebenszeit.

1.3 Zugriffskontrolle — Role-Based Access Control (RBAC)

Maßnahmen, die gewährleisten, dass ausschließlich berechtigte Personen auf die ihrem Berechtigungsprofil unterliegenden Daten zugreifen.

1.3.1 Granulare Rollenhierarchie

Die Plattform implementiert ein zweistufiges Berechtigungskonzept aus rollenbasierter (RBAC) und attributbasierter (ABAC) Zugriffskontrolle. Jede Berechtigung wird als signierte Policy im JWT-Token transportiert:

ROLLE	BERECHTIGUNGSUMFANG	TYPISCHER EINSATZ
Superadmin	Mandantenübergreifender Vollzugriff, God-Mode für Plattformadministration	Ausschließlich Pioneerdesk GmbH (Betreiber)
Tenant-Admin	Vollzugriff innerhalb des eigenen Mandanten: Monitoring, Alerting, Geräte, CMDB, ITSM, Befehlsausführung, Audit, Einstellungen, IAM, MSP-Verwaltung	IT-Leitung des Auftraggebers
Technician	Operativer Zugriff: Monitoring (Lesen), Alerting (Lesen/Schreiben), ITSM (Lesen/Schreiben), Befehlsausführung, Audit (Lesen)	IT-Mitarbeiter, Systemadministratoren
Tenant-User	Ausschließlich Lesezugriff auf alle Module. Keine Schreib-, Lösch- oder Ausführungsrechte.	Nicht-technisches Personal, Compliance-Prüfer

1.3.2 ABAC Policy Engine — Sicherheitsprinzipien

PRINZIP	UMSETZUNG
Default-Deny	Ohne explizite Erlaubnis wird jeder Zugriff verweigert. Es existiert keine implizite Berechtigung.
Deny-Override	Explizite Verweigerungen (`!resource:action`) überschreiben stets Erlaubnisse. Eine Deny-Policy kann nicht durch eine Allow-Policy aufgehoben werden.

Middleware-Enforcement	Jeder API-Endpunkt ist mit einer `RequirePolicy()` -Middleware geschützt, die **vor** Ausführung des Handlers die JWT-Policies gegen die erforderliche Berechtigung prüft. Bei unzureichendem Berechtigungsnachweis: HTTP 403 Forbidden — der Handler wird nicht aufgerufen.
Strikte Rollentrennung	Die Trennung zwischen Superadmin, Tenant-Admin, Technician und Tenant-User ist in der JWT-Signatur verankert. Eine Rechteeskalation erfordert die Ausstellung eines neuen, serverseitig signierten Tokens.

2. Trennungskontrolle — Kryptografische Mandantenisolation

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

2.1 Erzwungene Row-Level Security (RLS) auf PostgreSQL-Ebene

OneLog Enterprise implementiert die **strengste verfügbare Form der Mandantentrennung** innerhalb einer Multi-Tenant-Architektur: erzwungene Row-Level Security direkt auf der Datenbankebene.

Funktionsprinzip:

```
Authentifizierte Anfrage (JWT mit tenant_id)
 |
 +-- Middleware extrahiert tenant_id aus dem JWT
 |
 +-- iam.ScopedDB() setzt: SET LOCAL app.tenant_id = '<UUID>'
 |
 +-- Alle SQL-Abfragen innerhalb der Transaktion werden
 |   automatisch durch die RLS-Policy gefiltert
 |
 +-- Ergebnis: Mandant sieht ausschliesslich eigene Daten
     -> Unabhaengig von der Korrektheit der SQL-Abfrage
     -> Unabhaengig vom Anwendungscode
     -> Erzwungen durch die Datenbank selbst
```

SICHERHEITSEIGENSCHAFT	BESCHREIBUNG

FORCE ROW LEVEL SECURITY	RLS ist auf über **40 mandantenfähigen Tabellen** mit dem PostgreSQL `FORCE` -Flag aktiviert. Dieses erzwingt die Anwendung der Isolation **auch für Datenbankeigentümer und PostgreSQL-Superuser**. Es existiert kein Umgehungspfad auf Datenbankebene.
Automatische Kontextinjektion	Jede authentifizierte Anfrage setzt den Mandantenkontext als PostgreSQL-Session-Variable (`SET LOCAL app.tenant_id`). Sämtliche nachfolgenden Abfragen werden automatisch gefiltert.
Architektonische Garantie	Ein mandantenübergreifender Datenzugriff ist **systemisch ausgeschlossen** — selbst bei fehlerhaften SQL-Abfragen ohne WHERE-Klausel. Die Datenbank filtert eigenständig.
Safe-Fail	Fehlt der Mandantenkontext (z.B. durch einen Programmfehler), gibt die Datenbank **null Zeilen** zurück. Die Schutzwirkung bleibt auch im Fehlerfall bestehen.
Hintergrundprozesse	Systemdienste ohne Benutzerkontext (z.B. Heartbeat-Verarbeitung, KI-Agenten) verwenden explizite RLS-Bypass-Transaktionen (`SET LOCAL app.bypass_rls = 'on'`) — der Bypass ist pro Transaktion isoliert und endet automatisch mit dem Commit.

Geschützte Datenkategorien (Auszug aus 40+ Tabellen):

KATEGORIE	TABELLEN
Identitäts- und Zugriffsverwaltung	`users` , `roles` , `sessions` , `api_keys` , `policies`
Endgeräte und CMDB	`devices` , `installed_software` , `hardware_info` , `pending_commands` , `device_services` , `network_adapters` , `device_snapshots`
Monitoring und Alerting	`heartbeat_history` , `device_events` , `dex_scores` , `alert_rules` , `alert_history`
ITSM und KI-Automation	`tickets` , `ticket_comments` , `solver_solutions` , `ai_knowledge_base` , `tenant_ai_memory`
Compliance und Audit	`audit_logs` , `qa_audit_log` , `webhook_configs`
Sicherheit	`red_team_findings` , `software_packages` , `msp_branding`

2.2 Mandantenhierarchie mit referenzieller Integrität

```
Plattformbetreiber (Pioneerdesk GmbH)
 +-- Managed Service Provider (MSP)
      +-- Mandant (z.B. Klinikum -- Endkunde)
```

Datenbankseitige CHECK-Constraints und Fremdschlüssel stellen sicher, dass Mandanten stets einem übergeordneten MSP zugeordnet sind. E-Mail-Adressen sind mandantenspezifisch eindeutig (`UNIQUE (tenant_id, email)`). Die Mandantenlöschung kaskadiert vollständig über Fremdschlüssel (`ON DELETE CASCADE`).

3. Integrität

3.1 Weitergabekontrolle — Verschlüsselung

Maßnahmen, die gewährleisten, dass Daten bei der Übertragung und Speicherung nicht unbefugt gelesen, kopiert oder verändert werden.

3.1.1 Transportverschlüsselung (Data-in-Transit)

MASSNAHME	UMSETZUNG
Protokolle	Ausschließlich TLS 1.2 und TLS 1.3. Ältere Versionen (SSLv3, TLS 1.0, TLS 1.1) sind serverseitig deaktiviert.
Cipher-Suites	`HIGH:!aNULL:!MD5` — ausschließlich hochsichere Cipher-Suites. Server-Cipher-Präferenz erzwungen.
HSTS	`Strict-Transport-Security: max-age=31536000; includeSubDomains` — Browser werden für 12 Monate auf HTTPS festgelegt. Preload-fähig.
HTTP-Weiterleitung	Alle HTTP-Anfragen (Port 80) werden mit HTTP 301 auf HTTPS umgeleitet. Unverschlüsselte Kommunikation ist ausgeschlossen.
HTTP/2	Aktiviert für optimierte, multiplexierte Verbindungen.
Zertifikatsverwaltung	Let's Encrypt mit automatisierter Erneuerung (kein manueller Eingriff, kein Zertifikatsablauf).

3.1.2 Speicherverschlüsselung (Data-at-Rest)

MASSNAHME	BESCHREIBUNG
Datenbankverschlüsselung	AES-256 Verschlüsselung auf Volume-Ebene (STACKIT Managed PostgreSQL).
Backup-Verschlüsselung	Sämtliche Backups werden verschlüsselt gespeichert. Schlüsselverwaltung durch STACKIT.
MFA-Secret-Verschlüsselung	TOTP-Geheimnisse zusätzlich auf Anwendungsebene mit AES-256-GCM verschlüsselt (Defense-in-Depth).

3.1.3 Content Security Policy (CSP) und Sicherheitsheader

Sämtliche HTTP-Antworten werden durch eine restriktive Content Security Policy und ergänzende Sicherheitsheader geschützt (OL-SEC-012):

HEADER	WERT	SCHUTZWIRKUNG
Content-Security-Policy	`default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'; img-src 'self' data: blob:; font-src 'self'; connect-src 'self' wss://...; frame-ancestors 'self'; base-uri 'self'; form-action 'self'; object-src 'none'`	Vollständiger Schutz gegen XSS, Code-Injection und Clickjacking. Keine externen Skriptquellen. Kein Inline-JavaScript.
X-Content-Type-Options	`nosniff`	Verhindert MIME-Type-Sniffing
X-Frame-Options	`SAMEORIGIN`	Schutz vor Clickjacking / UI-Redressing
Referrer-Policy	`strict-origin-when-cross-origin`	Minimiert Referrer-Informationslecks
Permissions-Policy	`camera=(), microphone=(), geolocation=()`	Deaktiviert sensible Browser-APIs

3.2 Secrets Management — STACKIT Secrets Manager Vault

Alle sicherheitskritischen Schlüssel, Passwörter und API-Tokens werden zur Laufzeit aus dem **STACKIT Secrets Manager** (HashiCorp Vault-kompatibel) geladen. Es findet **keine** persistente Speicherung von Geheimnissen auf dem Dateisystem des Anwendungsservers statt.

Sicherheitsarchitektur des Secrets-Abrufprozesses:

```
Anwendungsstart (Boot)
 |
 +-- 1. Authentifizierung bei STACKIT Management Plane
 |      (RSA Key Flow mit Service Account Key)
 |
 +-- 2. Erstellung eines ephemeren Vault-Benutzers
 |      (Name: onelog-boot-YYYYMMDD-HHMMSS, ausschliesslich Leserechte)
 |
 +-- 3. Abruf aller benoetigten Secrets aus dem Vault
 |      -> Secrets verbleiben ausschliesslich im Prozess-Speicher (RAM)
 |      -> Keine Persistierung auf dem Dateisystem
 |
 +-- 4. Sofortige Loeschung des ephemeren Vault-Benutzers
 |      -> Verwaiste Benutzer bei Prozessabsturz: harmlos (nur Leserechte)
 |
 +-- 5. Anwendung startet mit gueltigen Secrets im Arbeitsspeicher
```

SICHERHEITSEIGENSCHAFT	UMSETZUNG
Zero-Disk-Persistence	Secrets existieren ausschließlich im RAM. Nach Prozessbeendigung unwiederbringlich gelöscht.
Ephemere Zugangsdaten	Pro Startvorgang ein dedizierter Vault-Benutzer (nur Leserechte). Sofort nach Abruf gelöscht.
Fail-Closed	Bei fehlgeschlagenem Secrets-Abruf (3 Versuche, exponentieller Backoff: 2s → 4s → 8s) terminiert der Prozess. **Die Anwendung startet nicht ohne gültige Geheimnisse.**
Zero-Trust-Logging	Es werden **niemals** Secret-Werte in Logdateien geschrieben — ausschließlich Schlüsselnamen.

3.3 Eingabekontrolle — Immutable Ledger (Digitaler Notar)

Maßnahmen, die gewährleisten, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt wurden.

OneLog Enterprise implementiert pro Mandant einen **Immutable Ledger** — ein kryptografisch verkettetes, manipulationssicheres Audit-Protokoll, das als **digitaler Notar** fungiert. Der Ledger kombiniert drei unabhängige Sicherheitsschichten:

1. **SHA-256 Hash-Kette** — Jeder Eintrag referenziert kryptografisch seinen Vorgänger. Die Manipulation eines einzelnen Eintrags invalidiert die gesamte nachfolgende Kette.
2. **CRYSTALS-Dilithium3 Postquanten-Signaturen** (NIST FIPS 204) — Sicherheitskritische Payloads werden mit dem postquantenresistenten Dilithium3-Verfahren digital signiert.

Eine Fälschung ist auch mit zukünftigen Quantencomputern rechnerisch ausgeschlossen.

3. **NIS2-Forensik-Narrative** — Jeder sicherheitsrelevante Audit-Eintrag enthält ein deutschsprachiges Klartext-Narrativ, das in die Hash-Berechnung einfließt. Diese Narrative sind manipulationssicher an den kryptografischen Beweis gebunden und dienen als gerichtsverwertbare Forensik-Dokumentation.

> **Roadmap Q3/2026: Migration auf hybride Signaturverfahren (Ed25519 + Dilithium3 kombiniert) gemäß aktueller BSI-Empfehlung (BSI TR-02102-1).**
> Das BSI empfiehlt derzeit, Post-Quantum-Kryptografie nicht als alleiniges Signaturverfahren einzusetzen, da die mathematischen Grundlagen noch vergleichsweise jung sind. Durch die hybride Kombination eines klassischen Verfahrens (Ed25519) mit dem PQC-Verfahren (Dilithium3) wird sichergestellt, dass die Integrität auch dann gewährleistet bleibt, falls in einem der beiden Verfahren eine Schwäche entdeckt wird.

Struktur eines Ledger-Eintrags:

FELD	BESCHREIBUNG
`id`	Eindeutige Kennung (UUID v4)
`tenant_id`	Mandantenkontext (RLS-geschützt — jeder Mandant besitzt eine eigene, vollständig isolierte Kette)
`user_id`	Handelnder Benutzer (NULL bei Systemaktionen)
`action`	Durchgeführte Aktion (z.B. `approve_draft` , `login` , `mfa_enabled`)
`entity_type` / `entity_id`	Betroffener Ressourcentyp und -kennung
`details`	Strukturierte Kontextdaten (JSON)
`nis2_narrative`	Deutschsprachiges Klartext-Forensik-Narrativ (in Hash gebunden)
`previous_hash`	SHA-256-Hash des vorherigen Eintrags (Kettenglied)
`current_hash`	`SHA-256(previous_hash || action || entity_id || nis2_narrative || RFC3339Nano(timestamp))`
`dilithium_signature`	CRYSTALS-Dilithium3 Postquanten-Signatur (2.701 Byte)
`created_at`	UTC-Zeitstempel mit Mikrosekunden-Präzision

Integritätsgarantien des Immutable Ledger:

MASSNAHME	UMSETZUNG

Kryptografische Verkettung	Jeder Eintrag enthält den SHA-256-Hash seines Vorgängers. Die Kette ist pro Mandant isoliert — ein Mandant kann weder die Existenz noch den Inhalt der Kette eines anderen Mandanten erkennen.
Genesis-Hash	Der erste Eintrag pro Mandant referenziert den definierten Nullwert (`0000...0000` , 64 Hex-Zeichen).
Serialisierung	PostgreSQL Advisory Locks (`pg_advisory_xact_lock`) erzwingen eine strikt sequenzielle Schreibreihenfolge pro Mandant. Race Conditions sind ausgeschlossen.
VerifyChain()	Vollständige Forward-Verifikation der gesamten Kette: repliziert jeden Hash, prüft Vorgänger-Referenz, verifiziert Dilithium3-Signaturen. Identifiziert exakt die Position eines gebrochenen Glieds. Jeder Mandant kann die Integrität seiner Kette jederzeit unabhängig prüfen.
Unveränderlichkeit	Die Audit-Tabelle besitzt **keine** UPDATE- oder DELETE-Endpunkte. Sie ist ausschließlich appendierend (INSERT-only).

Dilithium3 — Postquantensichere Signierung:

PARAMETER	WERT
Algorithmus	CRYSTALS-Dilithium Mode 3 (NIST FIPS 204, Cloudflare CIRCL-Implementierung)
Sicherheitsniveau	NIST Level 3 (äquivalent zu AES-192)
Öffentlicher Schlüssel	1.952 Byte pro Mandant
Privater Schlüssel	4.000 Byte (gespeichert im STACKIT Secrets Manager Vault)
Signaturgröße	2.701 Byte pro signiertem Payload
Einsatzgebiete	Audit-Einträge, Agent-Payload-Verifikation, Integritätsnachweis für Compliance-Audits

NIS2-Forensik-Narrative — Gerichtsverwertbare Dokumentation:

Jeder sicherheitsrelevante Vorgang wird mit einem deutschsprachigen Klartext-Narrativ dokumentiert, das **kryptografisch an den Hash gebunden** ist. Beispiele:

- *„Benutzer admin@klinikum.de hat Remediation-Skript 'Firewall-Regel für Port 445' am 2026-03-09T14:23:01Z zur Ausführung auf 12 Geräten freigegeben.“*
- *„KI-Agent AutoRemediator hat Patch KB5034441 als kritisch eingestuft. Human-in-the-Loop-Genehmigung durch tenant_admin@bank.de am 2026-03-09T15:01:33Z.“*

Diese Narrative sind manipulationssicher (Hash-gebunden) und dienen als Beweismittel für NIS2-Audits, Versicherungsfälle und gerichtliche Auseinandersetzungen.

Protokollierte Aktionen (Auszug): Benutzeranmeldung/-abmeldung, MFA-Aktivierung/-Deaktivierung, Passwortänderung, Lösungsfreigabe/-ablehnung, KI-Remediations-Genehmigung/-Ablehnung, Berechtigungsänderungen, manuelle Befehlsausführung auf Endgeräten, Geräteregistrierung/-löschung, Fleet-Update-Auslösung.

4. KI-Sicherheit — ITIL-basierte Mehrstufenarchitektur

> **Architektonisches Alleinstellungsmerkmal.**
> OneLog Enterprise ist nach unserem Kenntnisstand die einzige Endpoint-Management-Plattform, die KI-generierte Automatisierungsvorschläge durch ein mehrstufiges, ITIL-konformes Validierungssystem absichert: 16 spezialisierte KI-Agenten, ein Change Advisory Board (CAB) als Security Gatekeeper und ein obligatorisches Human-in-the-Loop-Genehmigungsverfahren.

4.1 Souveräne KI-Verarbeitung — Ausschließlich STACKIT EU

ASPEKT	UMSETZUNG
KI-Modell	Llama 3.3 70B (gehostet auf STACKIT EU-Infrastruktur, Cortecs-Partition)
Datenverarbeitung	Alle Prompts, Kontextdaten und KI-Antworten verbleiben auf deutschem Hoheitsgebiet.
Kein US-API-Zugriff	Seit Sprint 9 (KRITIS-Härtung) sind sämtliche nicht-europäische KI-Anbieter (Anthropic, Google, Groq, OpenAI) aus der Produktivkonfiguration entfernt.
Fallback-Kaskade	STACKIT EU (primär) → lokaler Ollama-Server (Fallback) → Template-Antwort (Fail-Safe). Kein Fallback auf US-Anbieter.
Mandantenisolation	KI-Agenten arbeiten mit expliziter Mandantenreferenz. Pro-Tenant-Token-Budgets verhindern Ressourcenmissbrauch.

Relevanz: Diese Architektur schließt den Datenabfluss an US-amerikanische KI-Anbieter **strukturell** aus — ein entscheidender Unterschied zu Wettbewerbern, die auf OpenAI/Azure AI oder AWS Bedrock aufsetzen und damit dem CLOUD Act unterliegen.

4.2 16-Agenten-Architektur mit ITIL-Personas

OneLog Enterprise betreibt **16 spezialisierte KI-Agenten** als verwaltete Hintergrundprozesse, koordiniert durch einen zentralen Orchestrator mit PostgreSQL-Job-Queue, LISTEN/NOTIFY-Echtzeitbenachrichtigung, Per-Agent-Circuit-Breakern und mandantenspezifischen Token-Budgets:

#	AGENT	ITIL-FUNKTION	PRIORITÄT
1	**AnomalyDetector**	ITIL Incident/Problem Manager — P1-P4-Triage, Root Cause Analysis, Problem Records	Critical
2	**ThreatCorrelator**	MITRE ATT&CK-Mapping, Kill-Chain-Analyse, IOC-Erkennung	Critical
3	**AutoRemediator**	Remediation-Vorschläge mit 8-Aktionen-Whitelist (Security Gatekeeper erzwungen)	Critical
4	**NIS2Auditor**	NIS2/BSI-Compliance-Prüfung	Normal
5	**ShadowITHunter**	Erkennung nicht genehmigter Software und Geräte	Normal
6	**PatchPrioritizer**	Risikobasierte Patch-Priorisierung	Normal
7	**CapacityPlanner**	Kapazitätsplanung und Trendanalyse	Batch
8	**TicketTriage**	Automatische Ticket-Klassifikation und -Priorisierung	Normal
9	**ExecutiveReporter**	Management-Reports und KPI-Dashboards	Batch
10	**NetworkAnalyst**	Netzwerkanomalien und Topologie-Analyse	Normal
11	**Copilot**	Interaktiver IT-Assistent (synchron, nicht Job-Queue)	On-Demand
12	**RedTeam**	Offensive Sicherheitsanalyse, MITRE ATT&CK-Simulation	Batch
13	**CAB Validator**	Change Advisory Board — Security Gatekeeper (Fail-Closed)	Critical
14	**LeadArchitect**	vCIO-Strategieagent mit persistentem Langzeitgedächtnis pro Mandant	Batch
15	**HiveMind**	Wissensextraktion aus gelösten Tickets → `ai_knowledge_base` (alle 6h)	Batch
16	**TechWriter**	Bilingualer Academy-Manual-Generator aus Changelogs (alle 2h)	Batch

4.3 Security Gatekeeper — Obligatorische CAB-Validierung

Der **Security Gatekeeper** ist eine architektonische Invariante: Jeder KI-generierte Remediationsvorschlag **muss** den CAB Validator passieren, bevor er einem Benutzer präsentiert wird.

Sicherheitsgarantien:

EIGENSCHAFT	BESCHREIBUNG
Kein Auto-Execute	KI-generierte Befehle werden **niemals** automatisch ausgeführt (KRITIS-Anforderung).
Kein Auto-Approve	Auch bei niedrigem Risiko erfordert jede Aktion menschliche Genehmigung.
Fail-Closed	Bei KI-Ausfall: Alle Remediations blockiert. System degradiert sicher.
Audit-Trail	Jede Genehmigung/Ablehnung wird im Immutable Ledger mit NIS2-Narrativ protokolliert.
Chain-Depth-Limit	Maximal 3 Agent-zu-Agent-Weiterleitungen. Verhindert Endlosschleifen.

4.4 Fail-Closed-Prinzip — Zusammenfassung

KOMPONENTE	BEI AUSFALL	VERHALTEN
CAB Validator	KI nicht verfügbar	**REJECT ALL** — Keine Aktion ohne CAB-Validierung
AutoRemediator	KI nicht verfügbar	Fallback: leere Aktionsliste + menschliche Genehmigung
Alle Worker-Agenten	KI nicht verfügbar	Regelbasierter Fallback (kein LLM-Zugriff erforderlich)
STACKIT LLM	Provider nicht verfügbar	Lokaler Ollama-Fallback → Template → Blockade
Secrets Manager	Vault nicht erreichbar	**Prozess terminiert** — Anwendung startet nicht

5. Hochperformante Datenverarbeitung — Write-Behind-Architektur

5.1 Heartbeat-Verarbeitung mit Redis Write-Behind

Für die echtzeitnahe Verarbeitung von Endgeräte-Heartbeats (Telemetrie: CPU, RAM, Disk, Netzwerk) setzt OneLog Enterprise eine **Write-Behind-Architektur** ein, die Sub-Millisekunden-Annahme mit zuverlässiger Persistenz kombiniert:

PARAMETER	WERT
Flush-Intervall	5 Sekunden
Batch-Größe	500 Heartbeats pro Flush
Deduplizierung	Letzter Heartbeat pro Tenant+Device (Map-basiert)
RLS-Bypass	Explizit pro Transaktion (`SET LOCAL app.bypass_rls = 'on'`), automatisch beendet bei Commit
Online-Status	Gerät gilt als „online“ wenn `last_seen < 5 Minuten`
Frontend-Aktualisierung	Automatisches Silent-Polling alle 15 Sekunden

6. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

MASSNAHME	UMSETZUNG
Container-Orchestrierung	Die zustandslosen (stateless) Anwendungs-Container werden via Docker orchestriert (`restart: unless-stopped`). Container-Ausfälle werden automatisch kompensiert.
Health-Check-Probes	PostgreSQL und Redis werden durch konfigurierte Health-Checks überwacht. Nicht erreichbare Dienste werden automatisch neu gestartet.

Datenpersistenz	Für die Datenpersistenz nutzen wir ausschließlich hochverfügbare **STACKIT Managed Services** (PostgreSQL/Redis) mit automatisierten Multi-AZ-Backups.
Netzwerkisolation	PostgreSQL und Redis sind ausschließlich über das interne Docker-Netzwerk erreichbar. Keine direkte Exposition gegenüber dem Internet. Kein externer Port-Exposure.
Redis-Härtung	Passwortauthentifizierung erzwungen (`requirepass`). Speicherlimit 256 MB mit LRU-Eviction.
Automatisierte Migrationen	Datenbankschema-Migrationen werden beim Serverstart automatisch, sequenziell und idempotent angewendet (aktuell 126 Migrationen). Die Datenbank ist stets konsistent mit der Anwendungsversion.
Secrets-Fail-Closed	Kann die Anwendung beim Start keine gültigen Secrets abrufen, terminiert der Prozess. **Die Anwendung startet nicht in einem unsicheren Zustand.**
Backup-Infrastruktur	STACKIT Managed PostgreSQL mit automatisierten, verschlüsselten Backups.

Definierte Wiederanlaufzeiten (Business Continuity):

- **RPO (Recovery Point Objective):**
  < 1 Stunde — maximaler tolerierter Datenverlust bei einem Ausfall.
- **RTO (Recovery Time Objective):**
  < 4 Stunden — maximale Dauer bis zur Wiederherstellung des Normalbetriebs.
- **Automatisierte Restore-Tests:**
  Quartalsweise Durchführung mit dokumentiertem Ergebnisprotokoll.

7. Continuous Security Auditing (DevSecOps)

OneLog Enterprise verfügt über eine **vollautomatisierte DevSecOps-Pipeline**. Jeder Code-Release wird durch kontinuierliche Sicherheitsanalysen nach internationalen Sicherheitsstandards auditiert, bevor er die Produktionsumgebung erreicht.

7.1 Automatisierte Sicherheitsanalyse (SAST/DAST)

STUFE	WERKZEUG	FUNKTION	FAIL-CLOSED
SAST	securego/gosec	Statische Analyse des Go-Quellcodes auf Injection-Flaws, Hardcoded Credentials, CWE/SANS Top 25. Severity-Filter: HIGH. Generiert JSON-Report (90 Tage Aufbewahrung).	**Ja** — Pipeline bricht bei HIGH/CRITICAL ab.
Dependency CVE	aquasecurity/trivy	Scannt `go.mod` -Abhängigkeiten (Backend) und `package.json` (Frontend) gegen die National Vulnerability Database (NVD). Severity: CRITICAL, HIGH.	**Ja** — `exit-code: 1` bei Fund. Deployment wird technisch blockiert.
SBOM	anchore/syft	Generiert Software Bill of Materials im CycloneDX-JSON-Format für Backend und Frontend.	Nein (informational).
Code-Signierung	DigiCert EV	Windows-Agent-Binary wird mit DigiCert EV Code Signing-Zertifikat (Pioneerdesk GmbH) signiert. Credentials aus STACKIT Secrets Manager.	**Ja** — unsignierte Binaries werden nicht ausgeliefert.

> **Fail-Closed-Prinzip:**
>
> Kontinuierliche SAST- und Dependency-Scans (gosec, trivy) sind in die GitHub CI/CD-Pipeline hart integriert. Die Pipeline agiert nach dem Fail-Closed-Prinzip: Bei Funden der Stufen HIGH oder CRITICAL wird das Deployment technisch blockiert. Das `deploy` -Job deklariert `needs: [security-scan]` — ohne bestandenen Security-Scan ist kein Deployment möglich.

7.2 Compliance-Standards und Prüfkataloge

STANDARD	BESCHREIBUNG	ANWENDUNGSBEREICH
OWASP Top 10 (2021)	Die zehn kritischsten Sicherheitsrisiken für Webanwendungen. Vollständige Abdeckung A01–A10.	Sämtliche API-Endpunkte, Frontend, Authentifizierungsflows
NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations.	Zugriffskontrolle (AC), Audit (AU), System Protection (SC), Integrity (SI)

NATO AC/322-D / STANAG 4774	Militärische Vorgaben für Sicherheitsbewertung von Informationssystemen.	Datenklassifikation, kryptografische Integrität, Mandantenisolation, Auditierbarkeit
CWE/SANS Top 25	Die 25 gefährlichsten Softwarefehler.	Quellcode-Analyse, Eingabevalidierung
BSI TR-02102	Kryptografische Verfahren: Empfehlungen und Schlüssellängen.	Passwort-Hashing (Argon2id), Signaturverfahren (Ed25519, Dilithium3)

7.3 Schwachstellen-Management und interne SLAs

SCHWEREGRAD (CVSS V3.1)	KLASSIFIKATION	MAXIMALE BEHEBUNGSFRIST	DEPLOYMENT-SPERRE
Critical (CVSS ≥ 9.0)	RCE, Auth Bypass	< 48 Stunden	**Ja** — Hotfix mit sofortiger Eskalation
High (CVSS 7.0 – 8.9)	Privilege Escalation, SQLi	< 7 Tage	**Ja**
Medium (CVSS 4.0 – 6.9)	XSS, CSRF	< 30 Tage	Nein (mit ISB-Risikoakzeptanz)
Low (CVSS < 4.0)	Informational	< 90 Tage	Nein

8. Organisatorische Maßnahmen (ISO 27001 Annex A)

8.1 Softwareentwicklung und Deployment

MASSNAHME	BESCHREIBUNG	ISO 27001 REFERENZ
CI/CD-Pipeline	Automatisierte Deployments über GitHub Actions. Code durchläuft Build-, Test- und Sicherheitsprüfung vor Produktivschaltung.	A.14 Systembeschaffung, Entwicklung und Wartung

Code-Signierung	Windows-Agentenbinaries mit DigiCert EV Code Signing-Zertifikat signiert. Extended Validation gewährleistet Herkunftsnachweis.	A.14.2 Sicherheit in Entwicklungsprozessen
Secret-Hygiene	Produktivsecrets ausschließlich im STACKIT Secrets Manager. Kein Secret in Quellcode oder Versionsverwaltung.	A.9.4 Zugangssteuerung für Anwendungen

8.2 Datensparsamkeit und Löschkonzept

MASSNAHME	BESCHREIBUNG	RECHTSGRUNDLAGE
Zweckbindung	Keine Verarbeitung über das für die Vertragserfüllung erforderliche Maß hinaus.	Art. 5 Abs. 1 lit. b DS-GVO
Automatische Bereinigung	Abgelaufene Tickets und temporäre Daten werden automatisiert gelöscht.	Art. 5 Abs. 1 lit. e DS-GVO
Kaskadierende Löschung	Mandantenlöschung kaskadiert vollständig über Fremdschlüssel: Benutzer, Geräte, Tickets, Lösungen, Audit-Logs.	Art. 17 DS-GVO

8.3 Personalmaßnahmen

MASSNAHME	BESCHREIBUNG	ISO 27001 REFERENZ
Vertraulichkeitsverpflichtung	Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet.	A.7.1 Vor der Beschäftigung
Sensibilisierung	Regelmäßige Schulungen zu Datenschutz und Informationssicherheit.	A.7.2 Während der Beschäftigung
Need-to-Know	Zugriffsrechte auf Produktivsysteme ausschließlich nach dokumentiertem Bedarf.	A.9.1 Zugangssteuerung

9. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Gemäß Art. 32 Abs. 1 lit. d DS-GVO.

9.1 Kontinuierliches ISMS (ISO/IEC 27001:2022)

VERFAHREN	FREQUENZ	DURCHFÜHRUNG	
Externes Überwachungsaudit	Jährlich	DICAS GmbH (akkreditierte Zertifizierungsstelle)	
Externe Re-Zertifizierung	Alle 3 Jahre	DICAS GmbH	
Internes ISMS-Audit	Halbjährlich	Informationssicherheitsbeauftragter (ISB)	
Management-Review	Jährlich	Geschäftsführung auf Basis des ISB-Berichts	
Risikobewertung (SoA-Review)	Mindestens jährlich, anlassbezogen	ISB in Abstimmung mit Geschäftsführung	
	Penetrationstest	**Mindestens jährlich** (Whitebox/Greybox) sowie anlassbezogen bei Major-Releases	Zertifizierte, unabhängige externe Dritte
Schwachstellenanalyse	Kontinuierlich	Automatisierter NVD-Mirror mit täglicher Synchronisation	

9.2 Technische Verifikationsverfahren

VERFAHREN	BESCHREIBUNG
Hash-Chain-Verifikation	Die Integrität des Immutable Ledger kann pro Mandant jederzeit über `VerifyChain()` vollständig verifiziert werden — inklusive Dilithium3-Signaturprüfung.
Automatisierte Health-Checks	Alle Infrastrukturkomponenten (Datenbank, Cache, Application Server) werden durch konfigurierte Probes überwacht.

CAB-Validator-Monitoring	Verfügbarkeit des Security Gatekeepers wird kontinuierlich überwacht. Bei Ausfall: automatische Fail-Closed-Aktivierung.

10. Zusammenfassung der Kontrollziele

KONTROLLZIEL (ART. 32 DS-GVO)	PRIMÄRE TECHNISCHE MASSNAHME	EVIDENZ / ZERTIFIZIERUNG
Vertraulichkeit	Sovereign Cloud (STACKIT BSI-C5), TLS 1.3, AES-256, Secrets Manager Vault (Zero-Disk-Persistence), AES-256-GCM MFA-Encryption	ISO 27001:2022, Zero CLOUD Act-Risiko
Integrität	Immutable Ledger (SHA-256 + Dilithium3 + NIS2-Narrative), Security Gatekeeper (CAB Fail-Closed), Human-in-the-Loop	NIS2-konformer digitaler Notar, postquantenresistent
Verfügbarkeit	Container-Orchestrierung, Health-Checks, Secrets-Fail-Closed, Write-Behind-Heartbeats, RPO < 1h / RTO < 4h	Automatisierte Wiederherstellung, STACKIT-Backup, quartalsweise Restore-Tests
Belastbarkeit	Row-Level Security (FORCE, 40+ Tabellen), ABAC Default-Deny, Ed25519-JWT (15min TTL)	Architektonisch unmögliche Cross-Tenant-Zugriffe
Pseudonymisierung	Mandantenspezifische UUIDs, kein Klartext-Logging	Zero-Trust-Logging-Policy
KI-Sicherheit	16 ITIL-Agenten auf Sovereign Cloud, CAB-Gatekeeper, Human-in-the-Loop, STACKIT EU only	Kein US-KI-Datenabfluss, Fail-Closed, Audit-Trail
Continuous Security	SAST-Pipeline, OWASP Top 10, NIST SP 800-53, NATO STANAG 4774, BSI TR-02102	NVD-Mirror, SBOM, SLA-Management
Regelmäßige Überprüfung	ISMS-Zyklus, externe Audits (DICAS), Hash-Chain-Verifikation, jährliche Pentests durch unabhängige Dritte	Jährliches Überwachungsaudit ISO 27001

11. Ansprechpartner

FUNKTION	KONTAKT
Auftragsverarbeiter	Pioneerdesk GmbH
Informationssicherheitsbeauftragter (ISB)	isb@pioneerdesk.one
Datenschutzanfragen	datenschutz@pioneerdesk.one
Technische Sicherheit	security@pioneerdesk.one
Zertifizierungsstelle	DICAS GmbH

Dieses Dokument ist Bestandteil der Auftragsverarbeitungsvereinbarung (AVV) gemäß Art. 28 DS-GVO zwischen der Pioneerdesk GmbH und dem Auftraggeber. Es wird bei wesentlichen Änderungen der technischen Architektur, des Rechtsrahmens oder auf Anforderung des externen Überwachungsaudits aktualisiert. Die jeweils aktuelle Fassung wird dem Auftraggeber auf Anfrage unverzüglich zur Verfügung gestellt.

Die Wirksamkeit der beschriebenen Maßnahmen wird durch das zertifizierte ISMS der Pioneerdesk GmbH (ISO/IEC 27001:2022, Zertifizierungsstelle: DICAS GmbH) kontinuierlich überwacht, bewertet und verbessert.

Dokumentenhistorie

VERSION	DATUM	ÄNDERUNG	FREIGABE
1.0	01.01.2026	Erstfassung	ISB
2.0	03.03.2026	Ergänzung KI-Sentinel, Postquantenkryptografie, Immutable Ledger, STACKIT Secrets Manager	ISB
3.0	03.03.2026	Neustrukturierung für KRITIS-PoC. ISO 27001:2022 als Zertifizierungsfundament.	ISB / GF
4.0	03.03.2026	Neuer Abschnitt: Continuous Security Auditing (DevSecOps). SAST-Pipeline, OWASP, NIST, NATO STANAG.	ISB / GF

5.0	09.03.2026	**Vollständiger Code-Audit und Korrektur.** Passwort-Hashing korrigiert (Argon2id statt Trinity Hash). JWT-TTL korrigiert (15min statt 24h). KI-Provider korrigiert (STACKIT EU only, keine US-APIs). Agenten-Architektur aktualisiert (16 statt 12). Neuer Abschnitt: Security Gatekeeper mit dreistufiger CAB-Validierung und Human-in-the-Loop. MFA AES-256-GCM Encryption ergänzt. NIS2-Forensik-Narrative dokumentiert. Write-Behind-Heartbeat-Architektur dokumentiert. CSP-Header dokumentiert. ITIL-Persona-Routing dokumentiert.	ISB / GF
5.1	09.03.2026	**DevSecOps-Tooling konkretisiert (Sprint 16).** Explizite Nennung der CI/CD-Pipeline-Werkzeuge (gosec, trivy, syft, DigiCert EV). Fail-Closed-Prinzip mit `needs: [security-scan]` -Dependency dokumentiert. SBOM-Generierung (CycloneDX) als Artefakt.	ISB / GF
6.0	**16.03.2026**	**CISO-Audit-Korrekturen:** (1) Klassifikation geändert auf ÖFFENTLICH / TLP:CLEAR. (2) Datenbank-Widerspruch behoben — Docker-Volumes durch STACKIT Managed Services ersetzt. (3) Post-Quanten-Roadmap für hybride Signaturen (Ed25519 + Dilithium3) ergänzt (BSI TR-02102-1). (4) Penetrationstests auf jährlich durch zertifizierte externe Dritte verschärft. (5) RTO/RPO und quartalsweise Restore-Tests definiert.	**ISB / GF**