GxP-Desk

FIT-CLEAN

CS-LEG-0006 · GXP-DESK DOCUMENTATION

Security Whitepaper.

FIT-only redaction. Effective 2026-06-04.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-LEG-0006	v1.0	2026-06-04	Legal & Compliance

Public — Documentation · Review cycle: On change

01 — DOCUMENT CONTROL

Control block and metadata anchor.

The control block identifies the document, its current revision, the regulated process it supports, and the people accountable for its lifecycle. Every value below is the source of truth for any downstream record, audit trail entry, or signature block.

DOCUMENT ID	CS-LEG-0006
TITLE	Security Whitepaper
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-06-04
REVIEW CYCLE	On change
DOCUMENT OWNER	Legal & Compliance
CLASSIFICATION	Public — Documentation
RELATED RECORDS	—
SUPERSEDES	— (initial release)

02 — APPROVALS

Sign-off table, ready for ink or e-signature.

The signatures below confirm review and authorisation of this document. Approvals must be recorded in chronological order. If the document is signed electronically, the e-signature record on the GxP-Desk platform supersedes any handwritten entry on this page and carries the same legal weight under 21 CFR Part 11 and EU GMP Annex 11.

Role	Name	Function	Date	Signature
Author		Validation Lead		
Reviewer		Quality Assurance		
Reviewer		Process / System Owner		
Approver		Head of Quality		
Approver		Regulatory Affairs		

03 — CONTENTS

What's in this document.

01 — WHAT THIS VERSION COVERS

What this version covers.

- **Multi-Tenant Architecture:** Logical isolation at the application layer (FK scoping), database layer (Row-Level Security), and audit-trail layer
- **Encryption Posture:** AES-256-GCM at rest (provider default), TLS 1.3 in transit (Caddyfile with Let's Encrypt)
- **Authentication & Access Control:** Custom JWT using jose, Argon2 password hashing, RBAC with permission guards, SoD enforcement; **MFA** (WebAuthn/Passkeys, TOTP, recovery codes); **SSO via SAML 2.0 and OpenID Connect** including enforcement, domain routing, and break-glass (NEW 2026-06-04)
- **Re-Authentication at Signing:** Step-up via MFAGrant (single-use, 5-minute window) on every electronic signature (NEW 2026-06-04)
- **BYOK & Encryption:** AES-256-GCM at rest (platform default); **BYOK** envelope encryption (per-tenant DEK, customer CMK) via AWS/Azure/GCP KMS including key rotation (NEW 2026-06-04)
- **Multi-Region Data Residency:** EU/US via `Tenant.dataRegion` with physically separated regional databases (NEW 2026-06-04)
- **Audit Trail:** Append-only AuditLog with sequenceNumber auto-increment, before/after snapshots, **tamper-evident hash chain v2** (Postgres immutability trigger, verify utility)
- **Session Management:** SessionTimeout component, document-lock function, document classification (Internal/Confidential/Secret)
- **Certifications:** ISO 27001, SOC 2 Type II, GDPR DPA, 21 CFR Part 11 / GMP Annex 11 / GAMP 5

02 — WHAT THIS VERSION DOES NOT COVER

What this version does NOT cover.

> **NOTE**
> Updated 2026-06-04: Multi-region data residency and BYOK are now implemented (see above) and have therefore been removed from this list.

- **SCIM 2.0 provisioning/deprovisioning** — no SCIM endpoint; identity lifecycle remains the customer's/IdP's responsibility
- **Audit-log streaming to SIEM** (Splunk/Datadog/S3) — webhooks are available, but there is no dedicated audit sink
- **X.509-/PKCS7-signed PDF exports** — integrity is instead ensured via the audit hash chain and the verification JSON

03 — DISCLAIMER

Disclaimer.

This whitepaper is a **reference document** for security and IT teams evaluating GxP-Desk. It is **not** a control list in the sense of a SOC 2 report or an ISO 27001 Statement of Applicability. For audited evidence, please request the SOC 2 Type II report and the ISO 27001 certificate under NDA.

Architecture: Multi-Tenant, Logical Isolation.

GxP-Desk is operated as a multi-tenant SaaS platform with logical isolation between accounts. Customer data is encrypted at rest and in transit; accounts and tenants are isolated at the application layer, the database layer, and the encryption-key layer.

Logical Isolation

- **Application Layer:** Every request carries an account/tenant scope; authorization is evaluated against the scope; cross-account requests are rejected.
- **Database Layer:** Per-account row-level isolation enforced by the platform; database queries are automatically scoped via `getAccountScopedDb()`, `getTenantScopedDb()`.
- **Encryption Key Layer:** Per-tenant data encryption keys (DEKs) under AES-256-GCM.
- **Audit Trail Layer:** Independent stream per account / tenant / system / change; cross-stream reads are rejected except for the account-level auditor.

05 — ENCRYPTION POSTURE

Encryption Posture.

Layer	Mechanism	Notes
In transit (Customer ↔ Platform)	TLS 1.3 (TLS 1.2 fallback for legacy IdPs)	Modern cipher suites, HSTS, Certificate Transparency
In transit (Intra-Platform)	Mutual TLS between services	Service identity validated, service-mesh enforcement
At rest (Data)	AES-256-GCM	Per-tenant DEKs; BYOK (customer CMK via AWS/Azure/GCP KMS, envelope encryption, key rotation)
At rest (Audit Trail)	AES-256-GCM (separate key domain)	Compromise of the data DEK does not decrypt the audit trail
At rest (Backups)	AES-256-GCM (separate key domain)	Cross-region replication

Identity and Access Control.

Authentication

- **Customer Users:** Custom JWT via jose; session-based auth with Argon2 password hashing. **SSO via SAML 2.0 / OpenID Connect** with enforcement and domain routing available; **MFA** via WebAuthn/Passkeys, TOTP, and recovery codes.
- **Re-Authentication at Signing:** Implemented — step-up via MFAGrant (single-use, 5-minute window) is enforced on every electronic signature.
- **GxP-Desk Personnel:** Only via support tickets with a documented reason; production access is break-glass.

Authorization

- **RBAC:** Four-level hierarchy (Account / Tenant / System / Change).
- **Permission Guards:** `requireAccountPermission()`, `requireTenantPermission()`, `requireChangePermission()` on server actions.
- **SoD Enforcement:** A phase-gate model enforces role separation across the change lifecycle (Requester ≠ Approver ≠ Signer).
- **Session Management:** SessionTimeout component, document lock in draft state.

Personnel Access to Customer Data

- **Routine Access:** None. Production access is break-glass via support ticket.
- **Break-Glass:** Requires a documented support ticket from the customer; logged in the account audit trail; time-bounded.
- **Scope:** Read-only by default.

Operations: Reliability & Recovery.

Availability

- **Deployment:** Multi-zone within region; automated failover.
- **Auto-Scaling:** Within capacity envelopes; load-tested before each major release.
- **SLA:** Per CS-MKT-0003, with concrete targets in the executed Service Order.

Disaster Recovery

- **Backup & Replication:** Cross-zone replication as the default.
- **RTO / RPO:** Per executed Service Order.
- **DR Testing:** Per SOC 2 Type II audit scope; reports available under NDA.

Monitoring

- **Application & Infrastructure Monitoring:** Availability and security monitoring through the hosting provider's toolset; on-call response by the GxP-Desk team.
- **Audit-Trail Capture:** AuditLog table with append-only discipline; manual review by tenant QA via the inspection view.

08 — APPLICATION SECURITY PRACTICE

Application Security Practice.

- **Secure Development Lifecycle:** Threat modeling, secure-coding guidelines, mandatory peer review.
- **Static Analysis & Dependency Scanning:** Gated in CI/CD.
- **Penetration Testing:** Annual external test (report under NDA).
- **Bug Bounty:** Responsible-disclosure program with documentation.
- **Secrets Management:** Managed secret store; rotation on a documented cadence.
- **Dependency Policy:** Third-party dependencies tracked; security review for new dependencies.

09 — COMPLIANCE & CERTIFICATIONS

Compliance & Certifications.

Certification	Scope	Evidence
ISO/IEC 27001:2022	ISMS covering development, operation, support	Certificate, Statement of Applicability (under NDA)
SOC 2 Type II	Common Criteria + Availability + Processing Integrity + Confidentiality + Privacy	Audited report (under NDA)
GDPR / UK GDPR	DPA in place; Art. 28 obligations implemented	DPA, technical & organizational measures
21 CFR Part 11 / EU GMP Annex 11 / GAMP 5	Domain-specific compliance for regulated customers	CS-CM-0001, CS-CM-0002, CS-CM-0003

10 — INCIDENT RESPONSE

Incident Response.

01 **Detect:** Monitoring + on-call response; customer-reported incidents via support; bug-bounty disclosures.

02 **Triage:** Severity classification per the incident-response procedure.

03 **Investigate:** Scoped investigation with a documented timeline and containment.

04 **Notify:** Affected customers per the DPA's notification clause and the MSA; DPA controllers per GDPR Art. 33 where applicable.

05 **Resolve:** Corrective actions; post-incident report under NDA where appropriate.

06 **Improve:** Lessons learned reviewed by management; corrective actions tracked.

11 — CODE REFERENCES

Code references.

- **JWT & Session Auth:** `lib/auth/jwt.ts` (jose 6.1.2), `lib/auth/password.ts` (Argon2 0.44.0)
- **Permission Guards:** `lib/auth/permissions.ts` (requireAccountPermission, requireTenantPermission, requireChangePermission)
- **Database Scoping:** `lib/db/scoped.ts` (getAccountScopedDb, getTenantScopedDb)
- **Audit Trail:** `prisma/schema.prisma` — `AuditLog` model with sequenceNumber, actionType, oldValue, newValue
- **Document Classification:** `prisma/schema.prisma` — `classification` field on Document (INTERNAL, CONFIDENTIAL, SECRET)
- **Session Management:** `components/auth/SessionTimeout.tsx`
- **TLS & HTTPS:** `caddy.conf` (Let's Encrypt configuration)
- **SSO:** `lib/sso/saml-client.ts`, `lib/sso/oidc-client.ts`, `lib/sso/enforcement.ts` (`SsoProvider`)
- **MFA & Re-Auth:** `lib/webauthn/*`, `lib/totp/*`, `lib/recovery-codes/*`, `MFAGrant` (step-up at signing)
- **BYOK:** `lib/byok/envelope.ts`, `lib/byok/providers/{aws-kms,azure-keyvault,gcp-kms}`, `TenantEncryption`, `KeyRotationEvent`
- **Multi-Region:** `lib/db/regions.ts`, `lib/db/multi-region.ts`, `Tenant.dataRegion`

REVISION HISTORY

Every change, tracked and signed.

Add one row for every controlled revision. Minor changes (typos, formatting) increment the patch version; substantive edits trigger a fresh review cycle and a new approver round.

Version	Date	Author	Summary of Change	Approver
1.0	2026-06-04	Documentation Team	FIT-only redaction limited to codebase-verified functionality.	Head of Documentation
—	—	—	Reserved for next revision. Do not delete this row.	—

GLOSSARY

Shared language, no ambiguity.

Definitions used throughout this document. Where a term has a specific meaning inside GxP-Desk, the platform-specific definition takes precedence over the generic regulatory term.

CSV	Computerized Systems Validation
GAMP 5	Good Automated Manufacturing Practice, Edition 5 (2nd edition, 2022)
GxP	Good 'x' Practice — covers GMP, GLP, GCP, GDP, GVP
IQ / OQ / PQ	Installation / Operational / Performance Qualification
Part 11	21 CFR Part 11 — US FDA rule on electronic records and electronic signatures
Annex 11	EU GMP Annex 11 — EU rule on computerised systems
URS	User Requirements Specification
FRS	Functional Requirements Specification
RTM	Requirements Traceability Matrix
SOP	Standard Operating Procedure
ALCOA+	Attributable, Legible, Contemporaneous, Original, Accurate (+ Complete, Consistent, Enduring, Available)
ICH Q9	International Council for Harmonisation Quality Risk Management guideline

— End of document —