ComplianceSuite

FIT-CLEAN

CS-LEG-0006 · COMPLIANCESUITE DOCUMENTATION

Security Whitepaper.

FIT-only redaction. Effective 2026-04-28.

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-LEG-0006	v1.0	2026-04-28	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	2026-04-28
REVIEW CYCLE	On change
DOCUMENT OWNER	Legal & Compliance
CLASSIFICATION	Public — Documentation
RELATED RECORDS	/output/CS-LEG-0006_Security_Whitepaper.pdf
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 ComplianceSuite 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 EDITION COVERS

What this edition covers.

- **Multi-Tenant Architecture:** Logical isolation at application layer (FK scoping), database layer (row-level security), 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 with jose 6.1.2, Argon2 password hashing, RBAC with permission guards, separation of duties enforcement
- **Audit Trail:** Append-only AuditLog with auto-increment sequence number, before/after snapshots
- **Session Management:** Session timeout 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

What this edition does NOT cover.

- **Multi-Region Data Residency** — no region field in codebase
- **BYOK (Bring Your Own Key)** — KMS/key vault integration not implemented

03 — DISCLAIMER

Disclaimer.

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

Architecture: Multi-Tenant, Logical Isolation.

ComplianceSuite 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, database layer, and encryption-key layer.

Logical Isolation

- **Application Layer:** Every request carries account/tenant scope; authorization is evaluated against 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 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, regularly rotated
At rest (audit trail)	AES-256-GCM (separate key domain)	Compromise of data-DEK does not decrypt 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 6.1.2; session-based auth with Argon2 0.44.0 password hashing.
- **Re-Authentication at Signing:** Not implemented — no second-factor challenge at sign operations required.
- **ComplianceSuite Personnel:** Only via support tickets with documented reason; production access is break-glass.

Authorisation

- **RBAC:** Four-level hierarchy (account / tenant / system / change).
- **Permission Guards:** `requireAccountPermission()`, `requireTenantPermission()`, `requireChangePermission()` on server actions.
- **SoD Enforcement:** Phase-gate model enforces role separation in change lifecycle (requester ≠ approver ≠ signer).
- **Session Management:** Session timeout 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 documented support ticket from customer; logged in 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 major release.
- **SLA:** Per CS-MKT-0003 with concrete targets in executed Service Order.

Disaster Recovery

- **Backup & Replication:** Cross-zone replication as 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 via the hosting provider's toolset; on-call response via the ComplianceSuite team.
- **Audit Trail Capture:** AuditLog table with append-only discipline; manual review by tenant QA via 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 programme with documentation.
- **Secrets Management:** Managed secret store; rotation on 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

Incident Response.

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

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

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

04 **Notify:** Affected customers per DPA's notification clause and 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.

Code Reference.

- **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 sequence number, action type, old value, new value
- **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)

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	2026-04-28	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 ComplianceSuite, 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 —