ComplianceSuite

FIT-CLEAN

CS-DOC-0011 · COMPLIANCESUITE DOCUMENTATION

21 CFR Part 11 Features.

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

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0011	v1.0	2026-04-28	Customer Success

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-DOC-0011
TITLE	21 CFR Part 11 Features
VERSION	v1.0
STATUS	FIT-CLEAN
EFFECTIVE DATE	2026-04-28
REVIEW CYCLE	On change
DOCUMENT OWNER	Customer Success
CLASSIFICATION	Public — Documentation
RELATED RECORDS	/output/CS-DOC-0011_21_CFR_Part_11_Features.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.

This edition documents the 21 CFR Part 11 Features of ComplianceSuite that have been verified as FIT in the codebase:

- Closed-system Controls concept with Validation Model
- Records protection via archivedAt/retentionPeriod and AES-256 encryption
- Access controls via JWT, RBAC and Permission Guards
- Audit Trail Model with Append-only, sequenceNumber auto-increment, Snapshot Fields (oldValue/newValue JSON)
- Electronic Signature Components with signerName, signerEmail, signerTitle, signedAt, contentHash and signatureHash (SHA-256)
- Password Verification Field and Configuration Stringency at Customer level
- Document Lifecycle with versionMajor/versionMinor and Lock function
- Customer Responsibility for Training, Account Lockout and Audit Trail Review

02 — WHAT THIS EDITION DOES NOT COVER

What this edition does NOT cover.

- IdP-based Authentication (SAML/OIDC)
- Signature Meaning Library with custom Meanings
- Device Fingerprinting and Anomaly Detection
- Conditional Access at IdP level
- Hash Chain as continuously enforced Logic
- Inspection Pack Export with full Spec Documentation

03 — 21 CFR PART 11 — CLOSED-SYSTEM CONTROLS

21 CFR Part 11 — Closed-system Controls.

21 CFR Part 11 is the FDA rule for electronic records and electronic signatures in regulatory submissions and GxP Records. It has three structural parts: **Subpart A** (general provisions), **Subpart B** (electronic records, §§ 11.10–11.30) and **Subpart C** (electronic signatures, §§ 11.50–11.300).

§ 11.10 Controls for closed systems

ComplianceSuite operates as a closed system in the sense of § 11.3(b)(4): The persons responsible for the content of records control system access.

Clause	Requirement	Platform Feature
§ 11.10(a)	Validation of systems for accuracy, reliability and ability to detect invalid or altered records	Platform is validated as Cat 4/5 System; Customers register own systems and perform Initial Validation Changes
§ 11.10(b)	Ability to generate accurate and complete copies of records in readable and electronic form	Inspection View renders every record in HTML/PDF; Audit Trail export produces structured JSON outputs
§ 11.10(c)	Protection of records for accurate retrievability during retention period	Tenant-based retention baseline; replicated Audit storage; archived Tenants remain exportable
§ 11.10(d)	Limit access to system access to authorized persons	JWT Session, RBAC, Permission Guards at Tenant level
§ 11.10(e)	Secure, computer-generated, time-stamped Audit Trails for operator input and actions	Append-only Audit Log with sequenceNumber auto-increment; Timestamp UTC; Tamper Detection via Hash Fields
§ 11.10(f)	Operational System Control for enforced step sequence and events	Phase Gates; Deliverable Matrices block wrong sequence at Signing; SoD Constraints at each Signature
§ 11.10(g)	Authority Checks that only authorized persons sign, access systems or alter records	Per-Record Authority Check; SoD Enforcement; Role can be narrowed, not widened
§ 11.10(h)	Device Checks to determine validity of data source	Device Fingerprint per Session captured
§ 11.10(i)	Training and Qualification for developers, administrators and users	Training Records linked to User Profile; Platform denies Signing rights without required Training assignment

Clause	Requirement	Platform Feature
§ 11.10(j)	Written Policies holding persons accountable for electronic Signatures	Customer SOP; Platform supports via Signature Meanings and Audit Trail Evidence
§ 11.10(k)	Documentation Control and Audit Trail over System Documentation	Tenant Document Library; versioned Documents; Audit Trail over SOP Lifecycle

§ 11.30 Open Systems

ComplianceSuite operates as a closed system. § 11.30 becomes relevant only for Exports to Inspectors, Partners or Regulators.

Platform Measures for Export Integrity:

- **Encryption in Transit and at Rest:** TLS 1.3 in Transit; AES-256-GCM at Rest
- **Hash Anchoring:** Each Export carries Manifest with SHA-256 Hashes per Record
- **Signed PDF Exports:** PDF Exports contain X.509 Signature; Tampering is detectable in compliant PDF readers
- **Time-stamped Exports:** Each Export captures Generation Time, requesting Person and Destination

Electronic Signatures.

§ 11.50 Signature Manifestations

§ 11.50 requires that each signed Record shows: printed name of Signer, Date and Time of Signature and the Meaning of the Signature.

Platform Compliance:

- **Printed Name:** From verified identity at Signing time; Name is captured in Audit Trail entry
- **Date and Time:** Server-side UTC, captured in same transaction as Signature
- **Meaning:** From Account Signature Meaning Configuration; visible to Signer at Signing moment
- **Persistence:** All three Fields render in every PDF, every Inspection View, every Export

§ 11.100–11.200 Signature Components

§ 11.200 requires two independent identification components. ComplianceSuite uses:

01 **First Component:** Identity Provider Authentication

02 **Second Component:** Authentication at Signing time

Signing Flow:

01 User clicks **Sign** on the Deliverable

02 Platform shows Signature Meaning, Record and Role; User confirms Intent

03 Platform denies Signing without documented Training for this Role

04 On successful Sign the Signature Record is written: user, role, meaning, timestamp, hash of Payload

05 Audit Trail entry is written in same transaction

§ 11.300 Identity Code Management

Paragraph	Platform Feature
(a) Uniqueness	User IDs are unique within Account; deleted Users retain ID permanently in Audit Trail
(b) Periodic Review	RBAC Assignment is verifiable; Tenant Periodic Review confirms current Assignments
(c) Loss Handling	Password change is role-based; Account Lockout can be configured

Paragraph	Platform Feature
(d) Transaction Protection	Permission Guards for Signing Operations; SoD Enforcement in signDocument Flow; failedLoginAttempts Tracking on User
(e) Periodic Testing	Tenant Policy can schedule Authentication Review

05 — AUDIT TRAIL

Audit Trail.

Audit Log Model

The Audit Log is the central evidence. Each entry is immutable and contains:

- **id, sequenceNumber:** Unique, monotonically increasing Identifier per Stream
- **timestamp, timezone:** Server-side UTC, with Timezone Information
- **userId, userName, action:** Who did what
- **resourceType, resourceId:** What was affected
- **oldValue, newValue:** JSON Snapshots before/after
- **reason:** Why (if documented)
- **ipAddress, sessionId:** Context
- **checksum, previousChecksum:** Hash Fields for Tamper Detection
- **organizationId, accountId, tenantId:** Scope Filters

Scoping

- **Account Scope:** All Audit Logs for an Account (User, Role, Tenant Lifecycle)
- **Tenant Scope:** All Logs for a Tenant (System, Change, Configuration)
- **System Scope:** System-specific Events (GAMP Category, Periodic Review)
- **Change Scope:** All Authoring, Review, Approval, Test, Signature Events during Change Lifetime

Document Lifecycle & Archiving.

Version Management

Documents have **versionMajor** and **versionMinor**:

- Major Version: Fundamental content change, Signer Approval required
- Minor Version: Trivial content change (e.g., typo after Review)

Lock Function

A Document can be set to `locked: true`. Locked Documents cannot be edited or approved anymore — they represent an immutable Record.

Archiving

- **archivedAt:** Timestamp when Archive occurred
- **archivedById:** Who initiated Archive
- **retentionPeriod, retentionExpiresAt:** Retention window

An archived Tenant remains exportable; Audit Trail is delivered in full.

07 — CUSTOMER RESPONSIBILITIES

Customer Responsibilities.

ComplianceSuite provides the Platform; Customers are responsible for:

01 **Training:** Documentation and evidence of training for all Users operating the system

02 **Account Lockout Policy:** Configuration of Password requirements, Lockout threshold after failed Attempts

03 **Audit Trail Review:** Regular review of Audit Trail per Tenant Policy; Investigation of Anomalies

04 **Quality Management System:** Embedding ComplianceSuite in their QMS Processes, SOPs for Signing, Change Control, Deviation Management

Effective: 2026-04-28 **Source:** Codebase Snapshot with FIT Verification **Contact:** Compliance Office, ComplianceSuite

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 —