GxP-Desk

FIT-CLEAN

CS-DOC-0011 · GXP-DESK DOCUMENTATION

21 CFR Part 11 Features.

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

DOCUMENT ID	VERSION	EFFECTIVE	OWNER
CS-DOC-0011	v1.0	2026-06-04	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	2026-06-04
REVIEW CYCLE	On change
DOCUMENT OWNER	Customer Success
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.

This version documents the 21 CFR Part 11 features of GxP-Desk that have been verified as FIT in the codebase:

- Closed-system controls concept with a validation model
- Records protection via archivedAt/retentionPeriod and AES-256 encryption (optional BYOK via AWS/Azure/GCP KMS, NEW 2026-06-04)
- Access controls through JWT, RBAC and permission guards; **SSO via SAML 2.0 / OpenID Connect** and **MFA** (WebAuthn/TOTP/recovery) (NEW 2026-06-04)
- Audit trail model with append-only design, sequenceNumber auto-increment, snapshot fields (oldValue/newValue JSON); **tamper-evident hash chain v2** with a Postgres immutability trigger (NEW 2026-06-04)
- Electronic signature components with signerName, signerEmail, signerTitle, signedAt, contentHash and signatureHash (SHA-256)
- **Re-authentication at signing** (step-up via MFAGrant, single-use, 5-minute window) and configuration strictness on the customer side (NEW 2026-06-04)
- Document lifecycle with versionMajor/versionMinor and a lock function
- Customer responsibility for training, account lockout and audit trail review

02 — WHAT THIS VERSION DOES NOT COVER

What this version does NOT cover.

NOTE

Updated 2026-06-04: SSO (SAML/OIDC), the consistently enforced hash chain and the inspection-pack export are now implemented and have therefore been removed from this list.

- Signature meaning library with user-defined meanings (currently a fixed enum)
- Device fingerprinting and anomaly detection
- Conditional access at the IdP level (customer/IdP responsibility)
- SCIM 2.0 provisioning/deprovisioning
- X.509/PKCS7-signed PDF exports
- Audit log streaming to SIEM (Splunk/Datadog/S3)

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

GxP-Desk is operated as a closed system within the meaning of § 11.3(b)(4): those responsible for the content of records control system access.

Clause	Requirement	Platform feature
§ 11.10(a)	Validation of systems for accuracy, reliability, and the ability to discern invalid or altered records	The platform is validated as a Cat 4/5 system; customers register their own systems and perform initial-validation changes
§ 11.10(b)	Ability to generate accurate and complete copies of records in human-readable and electronic form	The Inspection View renders every record in HTML/PDF; the audit trail export produces structured JSON output
§ 11.10(c)	Protection of records to enable accurate retrieval throughout the retention period	Tenant retention baseline; replicated audit storage; archived tenants remain exportable
§ 11.10(d)	Limiting system access to authorized individuals	JWT session, RBAC, permission guards at the tenant level; SSO (SAML/OIDC) with enforcement and domain routing
§ 11.10(e)	Secure, computer-generated, time-stamped audit trails for operator entries and actions	Append-only audit log with sequenceNumber auto-increment; UTC timestamp; tamper-evident hash chain v2 with a Postgres immutability trigger and Verify-Report
§ 11.10(f)	Operational system controls to enforce sequencing of steps and events	Phase gates; deliverable matrices block out-of-order signing; SoD constraints on every signature
§ 11.10(g)	Authority checks ensuring that only authorized individuals can sign, access systems, or alter records	Per-record authority check; SoD enforcement; a role can be narrowed but not widened

Clause	Requirement	Platform feature
§ 11.10(h)	Device checks to determine the validity of the data source	Not implemented: no device fingerprinting (only a "Remember this device" token); conditional access remains on the IdP/customer side
§ 11.10(i)	Training and qualification for developers, administrators and users	Training records are bound to user profiles; the platform denies signing rights without the required training assignment
§ 11.10(j)	Written policies that hold individuals accountable for electronic signatures	Customer SOP; the platform provides support via signature meanings and audit trail evidence
§ 11.10(k)	Documentation control and an audit trail over system documentation	Tenant document library; versioned documents; audit trail over the SOP lifecycle

§ 11.30 Open Systems

GxP-Desk is operated 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 (optional BYOK via AWS/Azure/GCP KMS)
- **Hash anchoring:** Every export carries a manifest with SHA-256 hashes per record as well as an `audit-chain-verification.json`
- **PDF export integrity:** PDF exports carry **no** X.509/PKCS7 signature; tamper evidence is provided through the audit hash chain and the verification JSON
- **Time-stamped exports:** Every export captures the time of generation, the requesting individual and the destination

04 — ELECTRONIC SIGNATURES

Electronic Signatures.

§ 11.50 Signature Manifestations

§ 11.50 requires that every signed record displays: the printed name of the signer, the date and time of signing, and the meaning of the signature.

How the platform satisfies this:

- **Printed name:** From the verified identity at the time of signing; the name is captured in the audit trail entry
- **Date and time:** Server-side UTC, captured in the same transaction as the signature
- **Meaning:** From the account signature-meaning configuration; visible to the signer at the moment of signing
- **Persistence:** All three fields render in every PDF, every Inspection View and every export

§ 11.100–11.200 Signature Components

§ 11.200 requires two independent identification components. GxP-Desk uses:

01 **First component:** Identity-provider or platform authentication (password or SSO)

02 **Second component:** Re-authentication at the time of signing — step-up via MFAGrant (single-use, 5-minute window), enforced on every signature

Signing flow:

01 The user clicks **Sign** on the deliverable

02 The platform displays the signature meaning, the record and the role; the user confirms intent

03 The platform denies signing without documented training for that role

04 On a successful sign, the signature record is written: user, role, meaning, timestamp, hash of the payload

05 The audit trail entry is written in the same transaction

§ 11.300 Identity Code Management

Paragraph	Platform feature
(a) Uniqueness	User IDs are unique within an account; deleted users retain their ID permanently in the audit trail
(b) Periodic review	RBAC assignment is verifiable; the tenant periodic review confirms current assignments

Paragraph	Platform feature
(c) Loss handling	Password changes are role-based; account lockout can be configured
(d) Transaction protection	Permission guards for signing operations; SoD enforcement in the signDocument flow; failedLoginAttempts tracking on the user
(e) Periodic testing	The tenant policy can schedule an authentication review

05 — AUDIT TRAIL

Audit Trail.

Audit Log Model

The audit log is the central record of evidence. Every 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 (where 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 and signature events during the change lifetime

Document Lifecycle & Archiving.

Version Management

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

- Major version: Fundamental content change, signer approval required
- Minor version: Trivial content change (e.g. a typo found after review)

Lock Function

A document can be set to `locked: true`. Locked documents can no longer be edited or approved — they represent an immutable record.

Archiving

- **archivedAt:** Timestamp of when archiving occurred
- **archivedById:** Who initiated the archiving
- **retentionPeriod, retentionExpiresAt:** Retention window

An archived tenant remains exportable; the audit trail is delivered in full.

07 — CUSTOMER RESPONSIBILITIES

Customer Responsibilities.

GxP-Desk provides the platform; customers are responsible for:

01 **Training:** Documenting and evidencing the training of all users who use the system

02 **Account lockout policy:** Configuring password requirements and the lockout threshold after failed attempts

03 **Audit trail review:** Regularly reviewing the audit trail in accordance with tenant policy; investigating anomalies

04 **Quality management system:** Embedding GxP-Desk into their QMS processes, with SOPs for signing, change control and deviation management

As of: 2026-06-04 **Source:** Codebase snapshot with FIT verification **Contact:** Compliance Office, GxP-Desk

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 —