FlightSense

Electronic Signatures, Recordkeeping & Data Protection

Compliance with FAA Advisory Circular 120-78B

This document describes how FlightSense satisfies the standards and guidelines in AC 120-78B for electronic signatures, electronic recordkeeping, and data protection as they apply to Part 141 flight training operations. It is intended for school administrators preparing for FAA acceptance of their electronic recordkeeping system and may be provided to FAA inspectors as supporting documentation during audits.

Under FAA rules, your school and course(s) are approved (e.g., your TCO and syllabi under Part 141), while an electronic recordkeeping system like FlightSense is "accepted" through a review process. When you submit a Letter of Intent (LOI) notifying your POI of your plan to use FlightSense and receive an authorizing Letter of Authorization (LOA) back, your system is formally accepted. This document provides the technical detail needed to support that acceptance.

1. Electronic Signatures

Ensuring authenticity, nonrepudiation, and immutability for training records that require formal sign-off.

Scope of Electronic Signatures

FlightSense applies formal electronic signatures to records where regulatory guidance requires certification or verification by an authorized instructor. Based on analysis of AC 141-1B and AC 120-78B, electronic signatures are applied at the stage check level—not at each individual lesson. This approach aligns with the AC 141-1B distinction between lesson-level training activities and formal evaluation checkpoints.

Records that receive a formal electronic signature include:

- Progress and stage check results (pass/fail with evaluating instructor sign-off)

Other training milestones—such as end-of-course test outcomes, course completion documentation, and enrollment events—are captured as electronic records with full metadata (who, when, and what was recorded) but do not pass through the electronic signing process. Where schools administer tests or generate certificates outside of FlightSense, those documents may be uploaded to the system and stored as part of the student's record.

Lesson-level training records (completion status, grades, instructor notes) are similarly captured as electronic records with per-entry audit metadata. Role-based access controls provide accountability at this level without imposing unnecessary workflow on instructors and students.

AC 141-1B §§ 3.12–3.14, 3.18 · AC 120-78B Ch. 2

Electronic Signature Implementation

FlightSense uses an electronic signature system for all records requiring formal sign-off. Each signature satisfies the eight key elements defined in AC 120-78B § 2.1.2:

AC 120-78B Requirement	FlightSense Implementation
Unique to the signer (§ 2.1.2.1)	Identifiers unique to each authenticated user
Means to identify and authenticate (§ 2.1.2.2)	Firebase Authentication with unique user ID; signer identity recorded
Under sole control of signer (§ 2.1.2.3)	Signing capability requires active authenticated session under the signer’s credentials
Executed with intent to sign (§ 2.1.2.4)	Deliberate action required — signer must review the record and confirm sign-off
Deliberate action (§ 2.1.2.5)	Explicit confirmation step; no auto-signing or batch-signing of records
Nonrepudiation (§ 2.1.2.6)	Event ID that permanently links the signer to the specific record content at signing time
Permanent and unalterable (§ 2.1.2.7)	Signature metadata (hash, timestamp, signer UID) is stored immutably; any record change is detectable via hash comparison
Document locked after signing (§ 2.1.2.8)	Hash verification detects post-signature modification; recordIntact flag indicates whether data remains unchanged

AC 120-78B § 2.1.2

Signature Notification

FlightSense notifies the signer upon successful application of an electronic signature, confirming in the application interface that the signature has been affixed to the record. When a signature is invalidated due to a superseding correction (per AC 120-78B § 2.2.8), the system notifies the affected signer that the prior signature has been invalidated and that re-signing is required.

AC 120-78B §§ 2.2.3, 2.2.8

Correcting Signed Records

AC 120-78B § 2.2.8 requires that an electronic signature be invalidated when a superseding entry is made to correct a record. FlightSense implements this directly: each electronic signature includes a superseded field and timestamp. When a correction is made, the original signature is marked as superseded (with a reference to the replacement signature), and a new signature is created over the corrected record. The original signature and its associated record content are preserved for audit purposes—nothing is deleted.

The signature verification system checks the electronic signature's record hash against current record data. A field indicates whether the signed data remains unchanged, providing a built-in integrity check at any time.

AC 120-78B §§ 2.2.7–2.2.8

2. Electronic Recordkeeping

Ensuring every training record captures complete, accurate, and tamper-evident data.

Key Elements of an Electronic Record

AC 120-78B § 3.1.1 defines the key elements that comprise a complete and valid electronic record. FlightSense captures all required elements for every training record entry:

AC 120-78B § 3.1.1	FlightSense Field(s)	Status
Type of event (§ 3.1.1.1)	Lesson type, check type, or endorsement type identifier	✓
Regulatory compliance info (§ 3.1.1.2)	Course module/subject, hours, pass/fail status linked to syllabus requirements	✓
Date and time (§ 3.1.1.3)	System-generated, tamper-resistant timestamps	✓
Location (§ 3.1.1.4)	Training facility linked at the organization level	✓
Personnel involved (§ 3.1.1.5)	Authenticated user IDs for student and instructor (assignment, creation, and updates)	✓
Certification/authentication (§ 3.1.1.7)	Electronic signatures on progress and stage checks	✓

AC 120-78B §§ 3.1–3.1.1

Audit Trail Design

FlightSense maintains a two-tier audit trail that reflects the regulatory distinction between lesson-level training activities and formal evaluation checkpoints:

Tier 1 — Lesson-Level Records. Every training record entry captures the identity of the user who created or modified the entry, along with system-generated timestamps. User identity is linked to the organization membership record, which tracks the user's role. This provides per-entry accountability—who did what and when—without requiring a formal signature at the lesson level.

Tier 2 — Signed Records. Progress and stage checks receive an electronic signature that binds the record content to the signer at a specific point in time. Any subsequent modification to the signed data is detectable through hash comparison, and corrections follow the superseding-entry process described in Section 1.

AC 120-78B §§ 3.2.1–3.2.2

Record Preservation and Immutability

AC 120-78B § 3.2.2 requires that records be preserved and unalterable without proper certification, verification, and/or authentication. FlightSense addresses this through multiple mechanisms: role-based access controls prevent unauthorized users from modifying records; signed records are locked upon signature and any modification triggers re-verification; and the system prevents data corruption through Firebase's transactional write model.

AC 120-78B §§ 3.2.1–3.2.4

3. Endorsement Records

FlightSense records endorsements for school documentation—it does not issue them.

Instructor endorsements required under 14 CFR Part 61 (solo flight, knowledge test, practical test, cross-country, etc.) must be given in the student's logbook—either physical or digital (e.g., ForeFlight). The actual endorsement signature and its associated regulatory requirements are the responsibility of the logbook system, not FlightSense.

FlightSense serves as the school's recordkeeping system for endorsements: it captures the fact that an endorsement was granted, by whom, and when, so the school maintains a complete training history for each student. Because FlightSense is acting as a recordkeeping system (AC 120-78B Chapter 3) rather than a signature system (Chapter 2), endorsement records do not require formal electronic signatures. They do, however, satisfy the key elements of an electronic record per § 3.1.1.

AC 120-78B § 3.1.1 Element	FlightSense Implementation
Who granted the endorsement	Instructor who granted the endorsement, linked to their certificate record
Who recorded the entry	May differ from the granting instructor in administrative scenarios
When	When endorsement was given and recorded in system
Record immutability	No update methods exist in the system—endorsement records can only be created or archived, never modified in place
Correction mechanism	Archive-and-recreate pattern: if a correction is needed, the existing record is archived with a reason and a new record is created, preserving the full audit trail

AC 120-78B § 3.1.1 · 14 CFR § 61.189

4. Data Backup & Disaster Recovery

Infrastructure safeguards that protect training records against loss, failure, or damage.

AC 120-78B § 3.2.7 requires that electronic recordkeeping systems include backup measures to maintain and provide access to records in the event of a system failure. FlightSense addresses this through a combination of cloud infrastructure safeguards and dedicated backup systems.

Database Records (Firestore)

Protection Layer	Detail
Point-in-time recovery	Continuous recovery capability with a 7-day window — allows restoration to any point within the prior 7 days
Daily snapshots	Automated daily backups with 30-day retention
Multi-region hosting	Firebase multi-region — data is automatically replicated across geographically separated data centers

File Storage (Student Documents)

Student documents stored in Firebase Storage (photo IDs, pilot certificates, medical certificates, TSA approvals, insurance documents) are protected through hourly delta backups to a geographically separate storage bucket. Because Firebase does not natively support file storage backups, FlightSense implements a custom backup function that captures changes on an hourly cycle, ensuring document recovery in the event of accidental deletion or system failure.

Disaster Recovery and Redundancy

The combination of multi-region hosting, point-in-time database recovery, daily snapshots, and hourly file backups provides a layered disaster recovery posture. Multi-region replication protects against regional outages. Point-in-time recovery enables restoration from data corruption. Daily and hourly backups provide additional recovery points.

It is important to distinguish backup (for disaster recovery) from retention (for regulatory compliance). The backup windows described above are designed to recover from system failures and data loss—they are not the record retention policy. Record retention is addressed in Section 5.

AC 120-78B §§ 3.2.5, 3.2.7

5. Record Retention

How long records are kept and the school's responsibility for regulatory retention periods.

FlightSense retains all electronic records indefinitely. There is no automatic purging of training records, endorsement records, signature records, or student data. Records persist in the system for as long as the school's account is active.

Under 14 CFR § 141.101, Part 141 schools are required to maintain current student training records and to retain records of graduated or terminated students for at least one year. Because FlightSense does not automatically delete data, schools using FlightSense satisfy this retention requirement by default—as long as records are not manually deleted by school personnel.

Schools should establish internal policies to ensure that records are not prematurely removed from the system. FlightSense's "Student Compliance Record Export" feature allows schools to generate comprehensive PDF exports of student records at any time, providing a secondary means of preserving records outside the electronic system.

14 CFR § 141.101 · AC 120-78B § 3.2.2

6. Access Control & Personnel Changes

Controlled access, role-based permissions, and procedures for personnel departures.

Role-Based Access Control

FlightSense implements role-based permissions that control what each user can view, create, and modify within the system. Each user has a unique authenticated account, and permissions are derived from their organizational role assignment. Signing capability (e.g., the ability to sign off on stage checks) is controlled by a specific permission that is tied to the instructor role.

AC 120-78B §§ 2.2.6, 3.2.1

Signature Revocation on Personnel Departure

AC 120-78B § 2.2.6.4 requires procedures to prohibit the use of an individual's electronic signature when they leave or terminate employment. FlightSense addresses this through the following process:

- **Role removal:** When an instructor departs, the school administrator removes their instructor role within FlightSense. This immediately revokes their signing capability, as the permission is no longer granted.
- **Account deletion:** If the user account is fully deleted, the system removes the user from all instructor-student relationships and deletes their Firebase Authentication account, preventing any future login.
- **Audit logging:** Role changes are tracked in an organization member audit log, which records the previous and current role assignments with timestamps.

Schools should document this process in their internal procedures manual so that it is available for inspector review. The recommended procedure: when an instructor departs, the chief flight instructor or designated administrator removes the instructor's role in FlightSense within the same business day. This constitutes the school's signature revocation procedure per § 2.2.6.4.

AC 120-78B § 2.2.6.4

7. Graduation Certificates

A deliberate paper-signature process for graduation documentation.

FlightSense automatically generates graduation certificates that include the school name, certificate number, student name, course, graduation date, and cross-country training statement. These certificates are exported as PDFs with a signature block for the chief instructor's handwritten signature.

This is a deliberate design decision. Because graduation certificates are typically printed and provided to the student as a physical document, applying a traditional handwritten signature ensures the certificate remains valid and verifiable regardless of whether the recipient has access to FlightSense's electronic verification system. The printed-and-signed approach is fully compliant with FAA requirements—AC 120-78B describes an acceptable means of using electronic signatures, but does not require them.

14 CFR §§ 141.85, 141.95 · AC 141-1B § 4.5

8. FAA Access & Inspection Readiness

Making records available to FAA and NTSB personnel.

AC 120-78B § 3.2.8.6 requires policies and procedures for making records available to the FAA and NTSB. FlightSense supports this through several mechanisms:

- **Student Compliance Record Export:** Generates comprehensive PDF exports including student information, course progress, chronological training logs, associated instructors, endorsements, and documents—available with one click for easy sharing and archiving.
- **Direct system access:** Schools may grant authorized FAA inspectors read-only access to FlightSense for the purpose of reviewing training records during inspections.
- **Printable records:** All electronic records can be printed or exported to PDF format for presentation in a manner acceptable to the requesting agency.

AC 120-78B § 3.2.8.6 · 14 CFR § 119.59

Appendix A — AC 120-78B Compliance Crosswalk

This table maps each relevant AC 120-78B requirement to FlightSense's current implementation, demonstrating readiness for FAA system acceptance.

AC 120-78B Reference	Requirement	Status
§ 2.1.2	Key elements of electronic signature	✓
§ 2.2.1	Signature uniqueness	✓
§ 2.2.2	Intent to sign	✓
§ 2.2.3	Notification of signed record	✓
§ 2.2.4	Scope of information / review before signing	✓
§ 2.2.5	Nonrepudiation	✓
§ 2.2.6	Security protocols and controlled access	✓
§ 2.2.6.4	Signature revocation on departure	✓*
§ 2.2.7	Signatures permanent and unalterable	✓
§ 2.2.8	Correction via superseding entry	✓
§ 2.2.9	Archivable	✓
§ 3.1.1	Key elements of electronic record	✓
§ 3.2.1	Controlled access	✓
§ 3.2.2	Record preservation	✓
§ 3.2.3	Protection of confidential information	✓
§ 3.2.4	Prevention of data corruption	✓
§ 3.2.5	IT system support / outage provisions	✓
§ 3.2.7	Backup measures	✓
§ 3.2.8.6	Records available to FAA/NTSB	✓

✓ = Meets acceptance criteria
✓* = Technical capability in place; school should document the procedure in their internal manual

Our Commitment:

Your success with FlightSense includes personal support through FAA acceptance and beyond.