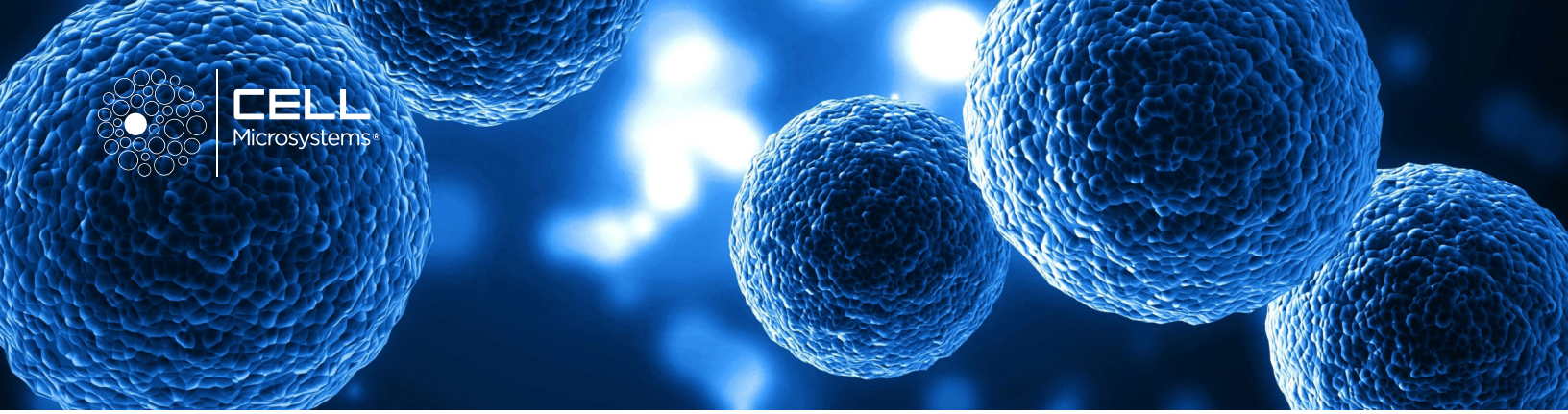

Cell Raft® AIR Compliance Features Supporting 21 CFR Part 11 Workflows

21 CFR Part 11 Compliance Module

Replace manual record keeping with a secure, inspection-ready electronic records system built into CellRaft AIR. Cryptographic audit trails, Windows-integrated authentication, and configurable electronic signatures - activated with a single license.

CellRaft AIR 21 CFR Part 11 Features

- Capture every user action in an immutable, SHA-256 protected audit trail
- Authenticate all users through your existing Windows domain - no separate credentials to manage
- Control system access with role-based permissions across 8 granular permission types
- Require electronic signatures for critical actions, with configurable policies per event type
- Export Array Records as certified copies (SQLite/TIFF) and export audit trails (PDF and CSV) for agency review
- Choose from a list of standardized signature meanings including Approval, Review, and Verification
- Deploy on a single workstation or multi-user server - both configurations validated on-premises
- Accelerate system validation with provided IQ/OQ/PQ protocol templates and SOP templates

Compliance-Ready, Without Compromise

The 21 CFR Part 11 module is a **licensed add-on** for CellRaft AIR Software v5.0. Compliance features are enforced at the service layer and centrally managed through the Administration interface. No passwords are stored in the CellRaft AIR database. All audit records are cryptographically integrity-checked on every retrieval.

CellRaft AIR 21 CFR Part 11 Implementation

Section	Requirement	Implementation
Audit Trail		
§11.10(e)	Secure, computer-generated, time-stamped audit trails; changes shall not obscure prior information	42+ event types; UTC timestamps; SHA-256 hash integrity; append-only storage; before/after values recorded
§11.10(a)	Validation - ability to discern invalid or altered records	SHA-256 hash calculated and verified on every audit record retrieval; automatic integrity failure detection
§11.10(b)	Generate accurate copies of records in human-readable and electronic form	PDF and CSV audit trail export; complete Array Record export as certified copy (SHA-256 validated SQLite and TIFF data)
§11.10(c)	Protect records for accurate and ready retrieval throughout the retention period	Immutable SQL Server storage; permanent retention; no auto-purge; PAGE compression for long-term efficiency
Electronic Records		
§11.1	Closed system controls for authenticity, integrity, and confidentiality	Windows domain authentication; TLS 1.2/1.3 encrypted gRPC; RBAC; no anonymous access
§11.10(d)	Limit system access to authorized individuals	Windows domain authentication + JWT session tokens + service-level RBAC on every operation
§11.10(g)	Authority checks - only authorized individuals can use the system or electronically sign	Permission-based service authorization; e-signatures require fresh Windows authentication independent of session state
§11.10(h)	Determine validity of the source of data input	Every data element attributed to a human user, instrument originator (AIR device), or automated system process
§11.10(i)	Personnel have education, training, and experience to perform assigned tasks	Implementor's Guide; IQ/OQ/PQ protocol templates; 5 SOP templates provided by Cell Microsystems
§11.10(j)	Written policies holding individuals accountable for actions under their electronic signatures	Authenticated Windows identity on all audit events; e-signatures enforce non-repudiation
§11.10(k)	Controls over system documentation and revision history	Version-controlled source code; formal release processes; Implementor's Guide documents all compliance features
Electronic Signatures		
§11.100(a)	Each electronic signature unique to one individual; not reused or reassigned	Windows domain enforces unique identity per user account
§11.200(a)	Non-biometric signatures shall employ at least two distinct identification components	Windows username + password; Windows Hello biometric supported as alternative
§11.200(a.1.ii)	Non-continuous signings shall employ all signature components	Fresh Windows authentication required for every e-signature; never cached between signing events
§11.300	Controls to ensure uniqueness, periodic review, and loss management of identification codes and passwords	No passwords stored in AIR; all credential controls delegated to Windows domain Group Policy and Active Directory
§11.50(a)	Signed records shall contain signer name, date/time, and signature meaning	Full signer name, UTC timestamp, and signature meaning recorded; stored with SHA-256 audit trail integrity
§11.70	Signatures linked to records; cannot be excised, copied, or transferred	SHA-256 hash cryptographically binds each signature to its audit event; database referential integrity prevents orphaned signatures

Cell Microsystems, Inc.

Product Information: cellmicrosystems.com/cellraft-air-systems/

Technical Support: cellmicrosystems.com/contact-us/support/

Contact Sales: cellmicrosystems.com/contact-sales/

Software Version: CellRaft AIR v5.0 — Document Version 1.0, February 2026 Specifications subject to change without notice. Organizations are responsible for ensuring their implementation meets all applicable regulatory requirements.

CELL Microsystems®

801 Capitola Drive, Suite 10
Durham, NC 27713
info@cellmicrosystems.com