

21 CFR Part 11 Readiness Statement

Document generated 2026-08-09 · Reflects the Aliquora production release current at that date · aliquora.com/docs/part-11-capability-matrix is the living version of this matrix

Scope and honesty note. This statement maps Aliquora's technical controls to the requirements of 21 CFR Part 11 and ALCOA+ expectations. Aliquora is not delivered pre-validated: computer-system validation in your environment, SOPs, training, and accountability policies are customer activities. Rows marked *Customer* identify them explicitly.

§11.10 — Controls for closed systems

REQUIREMENT	ALIQUORA CAPABILITY	STATUS
§11.10(a) — Validation of systems	Aliquora is built and tested for consistent performance. Formal computer-system validation (IQ/OQ/PQ) for your environment is a customer activity; the companion IQ/OQ/PQ protocol pack provides customer-executed templates.	Customer (templates provided)
§11.10(b) — Accurate and complete copies of records	Records (samples, results, audit logs) export to CSV; Certificates of Analysis and notebook entries export to PDF. Data is stored as structured, human-readable records.	Available
§11.10(c) — Protection of records for retrieval	Signed entries are protected from edits and audit entries are append-only; verified results change only via an explicit, password re-authenticated, reason-documented, audited administrator unlock. Long-term archival scheduling remains a customer responsibility.	Available (scheduling planned)
§11.10(d) — Limiting system access to authorized individuals	Authenticated accounts, role-based access control, account lockout after repeated failed logins, idle session timeout.	Available
§11.10(e) — Secure, computer-generated, time-stamped audit trails	Append-only audit log records user identity, action, affected resource, timestamp, and originating IP. Exports and verified-result unlocks are explicitly recorded. No interface exists to edit or delete entries.	Available
§11.10(f) — Operational checks enforcing step sequencing	Review and approval workflows enforce configurable step sequencing before reports are finalized.	Available
§11.10(g) — Authority checks	Role-based authority checks are enforced server-side on every protected request and at the point of signing.	Available
§11.10(h) — Device (terminal) checks	Not implemented.	Planned

REQUIREMENT	ALIQUORA CAPABILITY	STATUS
§11.10(i) — Personnel education, training, and experience	Personnel training and qualification is an organizational process; Aliquora's training/competency module can support the records.	Customer
§11.10(j) — Written accountability policies	An organizational policy matter; Aliquora's per-user signatures support enforcement.	Customer
§11.10(k) — Controls over systems documentation	Aliquora maintains its product documentation; control of your SOPs and validation documentation is a customer responsibility.	Customer

§§11.50–11.300 — Electronic signatures

REQUIREMENT	ALIQUORA CAPABILITY	STATUS
§11.50 — Signature manifestations	Each electronic signature captures the signer's identity, a timestamp, and the meaning of the signature (e.g. reviewed, approved, witnessed).	Available
§11.70 — Signature/record linking	Result signatures store a content snapshot bound by HMAC-SHA256 and are re-verified against the live record. Notebook-entry signatures pin a SHA-256 hash of the exact signed content; witnessing re-verifies the hash and is refused on any mismatch (tamper-evident).	Available
§11.100 — Signature uniqueness	Signatures are tied to unique, per-user accounts.	Available
§11.200 — Signature components & controls	Signing requires the user's session identity plus password re-authentication at the moment of signing; TOTP MFA is available as an additional factor. Witnessing requires a second individual's own credentials — self-witnessing is refused.	Available
§11.300 — Controls for identification codes/passwords	Unique usernames; bcrypt-hashed passwords; automatic lockout on repeated failures. Periodic password expiry policies are planned.	Partial (expiry planned)

Electronic laboratory notebook & inventory controls

REQUIREMENT	ALIQUORA CAPABILITY	STATUS
Two-person witnessed signing (ELN)	A notebook entry moves draft → signed → witnessed. Signing and witnessing each require password re-authentication; the witness must be a different user than the signer.	Available
Signature/content binding (ELN)	A SHA-256 hash of the exact content is pinned at signing and re-verified at witnessing; any change to the content refuses the witness signature.	Available
Amendments to signed entries	Signed entries reopen only through an amend action that requires a documented reason, preserves the signed version in the entry history, clears the signatures, and writes an audit event.	Available

REQUIREMENT	ALIQUORA CAPABILITY	STATUS
Controlled-substance witnessing (inventory)	Dispensing or disposing a controlled item requires a second organization member's credentials; the witness is recorded on the movement ledger row and in the audit trail. Self-witnessing is refused.	Available
Attachment integrity	Entry and sample attachments store SHA-256 checksums; uploads, downloads, and deletions are audited. Active-content file types are refused.	Available
Inventory ledger integrity	Every stock movement writes an append-only ledger row inside the same database transaction that updates the container, with row locking against concurrent dispensing; a reconcile check replays any container's ledger against its stored balance.	Available

Aliquora · aliquora.com · This document is provided for vendor-assessment purposes and does not constitute a certification. The capability matrix at aliquora.com/docs/part-11-capability-matrix supersedes this snapshot.