Countable Labs.

CFR 21 Part 11 requirement fulfillment for Countable Control Software

Countable Control Software includes features designed to support organizations in meeting federal requirements for electronic records under 21 CFR Part 11. See how the software's capabilities assist compliance efforts.

CFR Subsection	Summary of Requirement	Countable Labs Support	User Responsibility	Countable System Feature Support
§11.10(a)	System must be validated to ensure accuracy, reliability, consistent performance, and ability to detect invalid/altered records.	Provide validated software platform; tested functionality	Perform IQ/OQ procedures as documented in SOP	Validated software; secure authentication; audit trails; data integrity protections; documentation supporting IQ/OQ
§11.10(b)	System must generate accurate and complete copies of records in human-readable and electronic form.	Ensure software exports/ displays records	Confirm records meet internal SOPs	Structured, exportable experiment records
§11.10(c)	Records must be protected for retrieval throughout retention period.	Secure data storage & retention features	Configure retention & backups	Secure storage; configurable retention; easy retrieval
§11.10(d)	Limit system access to authorized individuals.	Role-based access & authentication	Assign/manage roles per SOPs	Login, role-based access control, configurable roles
§11.10(e)	Audit trails must record all changes/actions.	Tamper-evident, time-stamped logs	Review logs	Automated audit logging, linked to electronic signatures
§11.10(f)	Operational checks prevent invalid operations.	Implement system checks	Follow SOP workflow	Prevent logout mid-experiment; enforce checks
§11.10(g)	Authority checks enforce user-specific permissions.	Role-based access mechanisms	Assign/review roles	Configurable roles; periodic review support
§11.10(k)	Audit trail entries include user, timestamp, action, context; trails must be tamper-evident and secure.	Capture all system / experiment actions	Use audit trails	Full audit trail with context and tamper-evident logging
§11.50(a)	Signatures on records must include printed name, date/time, meaning.	Capture signature metadata	Ensure proper signature usage	Append electronic signatures
§11.50(b)	Signature must be linked to record and prevent changes.	Enforce immutable linkage	Ensure SOP compliance	Immutable linkage of signatures
§11.70	Signed records cannot be modified without audit documentation.	Enforce immutability	Ensure reports generated/ signed per SOPs	Signed reports are fully immutable; corrections require a new report
§11.100(a)	Signatures must be unique to one individual.	Ensure unique authentication	Assign unique users; prevent sharing	Unique authentication
§11.100(b)	Signatures cannot be reassigned or reused.	Prevent reuse/reassignment	Train users	System enforcement of unique signatures
§11.100(c)	Signatures require reason/comment for approvals/ rejections/modifications.	Prompt for reason/comment	Ensure correct rationale entered	Prompts and enforced entry
§11.200(a)(1)	Each electronic signature must include at least two components: user ID & password.	Enforce two-factor signature	Ensure credential security	User ID + password
§11.200(a)(1)(i/ii)	Re-entry of signature required for critical operations.	Enforce re-entry prompts	Re-enter signature	Prompted re-entry
§11.200(a)(2)	Restrict signing to authorized users with proper roles.	Enforce role-based signing	Assign correct roles	Role-based signing control
§11.200(b)	Signatures must be permanently linked to the record.	Enforce immutable linkage	Ensure records signed properly	Permanent linkage
§11.300(a)	Unique assignment of credentials; prohibit sharing.	Enforce unique logins	Maintain individual accounts; do not share	Unique accounts; login authentication
§11.300(b)	Mechanism to report lost/compromised credentials; remediation & logging.	Provide workflow for reporting/ resetting credentials	Report lost credentials; follow SOPs	Admin has disable/reset permissions; all actions logged
§11.300(c)	Biometric/hardware tokens controlled by admin; periodic verification.	Support optional tokens	Admin assigns/activates/ verifies devices	Optional device support with audit trail
§11.300(d)	Password controls: prevent reuse, enforce secure storage.	Enforce password history & secure storage	Configure policies	Configurable expiration/history; hashed storage
§11.300(e)	Periodic review of user access & permissions.	Provide reporting on accounts/ roles	Conduct access review per SOPs	Generates user/account reports