Version Control - TotalLab

21 CFR Part 11 Compliance Guide

Introduction

This document presents the technical features of Version Control in regards to 21 CFR Part 11 subpart B - Electronic Records and how these individual regulations can be satisfied and help your organisation comply with the Food and Drug Administration's (FDA) 21 CFR 11 regulations.

Each regulation is translated and explained for a more easy-to-read document. We outline how Version Control and the customer organisation share responsibilities for achieving compliance.

Before reading the document please note that the explanations we provide represent our interpretations of the 21 CFR Part 11 regulations. We do not represent any government agency and nothing in the in this guide should be taken as fact. The regulations we provide are true to the publishing date.

Version Control is intended to address GLP/GMP requirements in compliance with 21 CFR part 11. It is the user's responsibility to ensure that the software is appropriately validated within the context of the user's particular environment, and to ensure that the other Part 11 compliance elements are implemented appropriately.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Interpretation

How an organisation validates that the data produced from a system can be trusted.

How Version Control complies	All TotalLab software is adequately tested and follows a documented software life-cycle process.
Responsibilities of an organisation using Version Control	Validating the software for its intended use, ensuring it performs in their environment correctly.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

Interpretation

The ability for an organisation to generate complete records that an agency/auditor can review and copy. These are to be provided in a format for human to read and understand and in electronic format.

How Version Control complies

Version Control generates a date and time-stamped image history audit trail which records all action regarding the software usage (E.g. who and when image projects have been opened, read-only and approved..

These audit trails are made available in PDF format for read only inspection and can be stored on the server to allow IT administrators or QA managers easy access.

Responsibilities of an organisation using Version Control

The customer organisation is responsible for restricting physical access to the secure folder and ensuring reports are stored and accessible for review.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Interpretation

How an organization protects documentation and keeps it readily available for a suitable record retention period.

How Version Control complies	Records are stored securely on the Version Control server. • Version control will not analyse or store corrupted data (altered outside of the system).
Responsibilities of an organisation using Version Control	The customer organisation is responsible for defining a record retention period as part of a GxP regulated process.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(d) Limiting system access to authorized individuals.

Interpretation

How an organisation ensures that authorized only people have access to the system.

How Version Control complies

Access to Version Control is limited to users with a valid user-name and password (electronic signature).

Additional security includes:

- Disabling projects being analysed or viewed by another user.

Responsibilities of an organisation using Version Control

The customer organisation is responsible for designating which users are allowed access to Version Control.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(e) Use of secure, computer- generated, time, stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Recorded changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Interpretation

How an organisation ensures that the complete audit trail history of a project is captured by a the system and retained for the appropriate amount of time, and viewable by humans.

How Version Control complies

Version Control allows secure, time stamped audit trail records to be generated automatically.

- Image history audit trail – time and date-stamped records showing all experiment actions. (E.g. who and when images have been opened and signed off).

Audit trails can be exported to a .pdf for read only inspection/ viewing.

Responsibilities of an organisation using Version Control

The customer organisation is responsible for deciding what the data retention period is.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate

Interpretation

How an organization makes sure that electronic workflows in computer systems function correctly.

How Version Control complies	Life-cycle checks to disable certain actions based on state of project. Once a electronic signature is attached to a record, the record can no longer be modified by an unauthorised personnel.
Responsibilities of an organisation using Version Control	Version Control allows any software to be used therefore we cannot restrict or guarantee the order of actions to be completed in a certain over with the organisations chosen software.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Interpretation

How an organization limits user access (system level and record level) and verifies that the users performing functions in the system are authorized to do so.

How Version Control complies	Access to the record level is restricted to authorized individuals only with valid user-names and passwords. Version Control prevents users from performing actions which have not been granted access to.
Responsibilities of an organisation using Version Control	Permissions granted to individual users are the responsibility of the customer organisation. It is the customer organisations responsibility to grant privileges to users on a system level.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(h) Use of device (E.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction

Interpretation

How an organization verifies that equipment being used for regulatory purposes is valid.

How Version Control complies	This is not applicable as it involves technical controls that must be implemented by the customer organisation.
Responsibilities of an organisation using Version Control	Standard operating procedures should be in place to cover operation of equipment in a GMP environment.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Interpretation

How an organisation makes sure only trained and qualified people perform functions on or within the system.

How Version Control complies	This is not applicable as it involves technical controls that must be implemented by the customer organisation.
Responsibilities of an organisation using Version Control	It is the customer's responsibility to ensure that there are polices in place to ensure that the person(s) who develop, maintain or use the electronic records have the education and training to perform their assigned tasks.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Interpretation

How an organization holds individuals accountable for the integrity of their actions related to electronic records and electronic signatures.

How Version Control complies	This is not applicable as it involves controls that must be implemented by the customer organisation.
Responsibilities of an organisation using Version Control	It is the customer's responsibility to ensure that there are polices in place to adhere to the actions initiated under the electronic signatures are met.

Subpart B - Electronic Records
Sec. 11.10 Controls for closed systems.

Regulation

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Interpretation

How an organisation controls documents related to system operation and maintenance and preserves the complete history of changes made to these documents.

How Version Control complies	Processes are in place to ensure that access to TotalLab version control user documentation is supplied and updated and distributed as necessary.
Responsibilities of an organisation using Version Control	Customer is responsible for distributing user documentation to the relevant personnel.

Subpart B - Electronic Records
Sec. 11.50 Signature Manifestations

Regulation

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature

Interpretation

Any time an electronic record is signed, the following information must be visible and associated with the signature:

(1) Printed name of signer

(2) Date and time of signature

(3) Meaning of signature (E.g. approval of data calculations)

How Version Control complies	Audit reports show (1) Full printed name is recorded. (2) Date and time of the electronic signature is recorded. (3) A reason for approval is recorded along with the signatures.
Responsibilities of an organisation using Version Control	The customer organisation must properly configure users names to include a list of full names. The customer organisation must assign a SOP for including valid reasons for approval or disapproval.

Subpart B - Electronic Records
Sec. 11.50 Signature Manifestations

Regulation

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Interpretation

The three bullets of data above are also subject to Part 11 and must be in human-readable format.

How Version Control complies	Audit report and analysis reports are stored as human-readable PDF.
Responsibilities of an organisation using Version Control	Not applicable.

Subpart B - Electronic Records
Sec. 11.70 Record and Signature Linking

Regulation

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means

Interpretation

Any kind of signature (ink or electronic) executed to an electronic record must remain connected to that record forever. It can't be removed, covered over, erased, transferred, etc.

How Version Control complies	Version Control has security access to users with a valid user-name and password (electronic signature). Electronic signatures attached to an electronic record are reported and those records cannot be altered or deleted.
Responsibilities of an organisation using Version Control	Not applicable.

Subpart B - Electronic Records
Sec. 11.100 General Requirements

Regulation

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Interpretation

Each person must have a unique electronic signature that has never been and never will be used by anyone else.

How Version Control complies	Duplicate user-names are not allowed in Version Control.
Responsibilities of an organisation using Version Control	The customer organisation must properly configure users so that each user has a historical unique signature. The customer organisation should keep a list of user IDs to prevent reissue or reuse of user ID,. Version Control does not allow group logins.

Subpart B - Electronic Records
Sec. 11.100 General Requirements

Regulation

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual

Interpretation

Before a user can use an electronic signature, their identity must be verified.

How Version Control complies	This is not applicable for this application as it involves technical and procedural controls that must be implemented by the customer organisation.
Responsibilities of an organisation using Version Control	Standard operating procedures should be in place for verifying an individual's identity.

Subpart B - Electronic Records
Sec. 11.100 General Requirements

Regulation

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Interpretation

Before a user can use an electronic signature, their identity must be verified. The organisation must notify the FDA of the electronic signature and its intention as legally binding as ink signatures. The first step in the process is to write and mail the FDA a paper letter signed with ink signatures.

The organization must provide that the electronic signatures are legally binding if the FDA asks for proof.

How Version Control complies	This is not applicable for this application as it involves technical and procedural controls that must be implemented by the customer organisation.
Responsibilities of an organisation using Version Control	The customer organisation should send a letter to the FDA with this confirmation of electronic signatures.

Subpart B - Electronic Records
11.200 Electronic Signature Components and Controls

Regulation

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

Interpretation

Electronic signatures that are not biometric.

(1) Must be made up of at least two distinct parts (e.g. user-name and password).

How Version Control complies	The user login (electronic signature) contains both a user name and password.
Responsibilities of an organisation using Version Control	The customer organisation is responsible for configuring the electronic signature in accordance with the guidelines.

Subpart B - Electronic Records
11.200 Electronic Signature Components and Controls

Regulation

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

Interpretation

The first time a user signs a record after logging into a system, the system must require them to enter ALL of the parts of their signature (i.e., user ID and password). Subsequent signings during that same session only require the use of ONE part (i.e., password).

How Version Control complies	An electronic signature (user-name and password) is required at login to TotalLab Version Control. Subsequent signings require a password.
Responsibilities of an organisation using Version Control	Configuring the system so that an electronic signature is required at the first signing and any subsequent signings require at least one component.

Subpart B - Electronic Records
11.200 Electronic Signature Components and Controls

Regulation

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components

Interpretation

Each time a user logs out and logs back in (or gets timed out by the system), the clock restarts and the first record signed after logging in must require ALL parts of the signature.

How Version Control complies	Not applicable.
Responsibilities of an organisation using Version Control	The customer organisation must properly configure user accounts to enable automatic lock out after a user is inactive for a period of time.

Subpart B - Electronic Records
11.200 Electronic Signature Components and Controls

Regulation

(2) Be used only by their genuine owners; and

Interpretation

Electronic signatures must only be used by the individuals to whom they are assigned.

How Version Control complies	Version Control prevents the creation of duplicate user names.
Responsibilities of an organisation using Version Control	The customer organisation must properly configure user accounts in Windows. (e.g. list of user IDs to prevent reissue or reuse of user ID) The customer organisation must properly ensure the security of user names and passwords.

Subpart B - Electronic Records
11.200 Electronic Signature Components and Controls

Regulation

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Interpretation

If an individual's electronic signature must be used by someone it's not assigned to, the system must require at least two people to work together to do so.

How Version Control complies	At least two users must work together to use another persons signature. These users must be verified by the software to use the emergency login. All actions are recorded in the audit trail.
Responsibilities of an organisation using Version Control	The customer organisation must properly ensure that two or more signatures of individuals are provided if an electronic signature must be used by someone it was not assigned to.

Subpart B - Electronic Records
11.200 Electronic Signature Components and Controls

Regulation

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Interpretation

Electronic signatures that are biometric (E.g., fingerprint scan, retinal scan) can only be used by the individuals to whom they are assigned.

How Version Control complies	Not applicable. Version Control does not support biometric electronic signatures.
Responsibilities of an organisation using Version Control	Not applicable.

Subpart B - Electronic Records
11.300 Controls for identification codes/passwords.

Regulation

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

Interpretation

For electronic signatures that make use of identification codes (i.e., user-names and passwords) the following controls need to be in place:

No two users can have the same combination of user ID and password – each combination must be unique – and each user ID can only be assigned to one individual, historically.

How Version Control complies	Version Control prevents the creation of duplicate user names.
Responsibilities of an organisation using Version Control	The customer organisation is responsible for maintaining this uniqueness.

Subpart B - Electronic Records
11.300 Controls for identification codes/passwords.

Regulation

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (E.g., to cover such events as password aging).

Interpretation

Passwords must be checked, recalled, or changed from time to time.

How Version Control complies	You can specify an expiry date of passwords used in TotalLab Version Control.
Responsibilities of an organisation using Version Control	It is the customer's responsibility to configure windows accounts so that passwords can expire within a time frame according the companies policies.

Subpart B - Electronic Records
Sec. 11.300 Controls for identification codes/passwords.

Regulation

(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls

Interpretation

If a password/ identification device is lost or stolen, it must be de-authorized and a secure replacement must be issued.

How Version Control complies	Not applicable. It is the customer's responsibility to have a SOP on system and password security and access control.
Responsibilities of an organisation using Version Control	The customer organisation must properly configure user accounts for access to delete users accounts and reset passwords.

Subpart B - Electronic Records
Sec. 11.300 Controls for identification codes/passwords.

Regulation

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organisational management

Interpretation

Unauthorized attempts to access user IDs or passwords/pass-codes must be detected and reported to the appropriate person/group in the organisation for investigation.

How Version Control complies	All login attempt fails are recorded in the audit trail in real time for further investigation.
Responsibilities of an organisation using Version Control	The customer organisation must properly configure Windows user accounts on the operating system.

Subpart B - Electronic Records
Sec. 11.300 Controls for identification codes/passwords.

Regulation

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner

Interpretation

Pass-code tokens must be tested before they are issued for use and periodically while in use to make sure they're functioning correctly.

How Version Control complies	Not applicable. Testing of identification codes falls under the responsibilities of the customers organisation.
Responsibilities of an organisation using Version Control	This issue is not applicable for this compliance analysis as it involves technical and procedural controls that must be implemented by the customer.