Guidance on 21 CFR Compliance for **firefly**® Software Version 1.8

Introduction

Compliance with regulations set forth by the Food and Drug Administration (FDA) in 21 CFR Part 11, as well as other pertinent guidelines like Annex 11 from the European Commission, requires a collaborative effort between computerized system vendors and their customers. It's imperative to recognize that compliance isn't solely achieved through software but rather through the seamless integration of software tools and established administrative procedures.

firefly Software Version 1.8 offers a suite of tools aimed at streamlining and expediting compliance with 21 CFR Part 11. This document provides an overview of the features and tools included in firefly Software Version 1.8 by SPT Labtech, with specific focus on relevant sections of 21 CFR Part 11.

Controls for Closed System

21 CFR Part 11 Reference	Responsibility (Control)	Explanation
11.10 Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.	User with help from SPT Labtech	SPT Labtech firefly software is a closed system. SPT Labtech delivers support with user training. In the system, features that ensure authenticity of electronic records can be activated. Selection of this feature can only be adjusted with super user level access. Automated protocol verification is available within the software to ensure the functionality of the instrument within defined parameters.
11.10 (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	User with help from SPT Labtech	The user must have procedures, such as Standard Operating Procedures (SOPs) and Work instructions (WIs) in place for appropriate validation and operation of the system. SPT Labtech can deliver support with User training, IQ and OQ services. System Audit trails are available to track alterations to protocols and records.
11.10 (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.	SPT Labtech (Technical) User (Procedural)	Protocol Reports and audit trails can be displayed on screen and exported to standard 3rd party software tools.

11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	SPT Labtech (Technical) User (Procedural)	All data generated with the firefly system is stored and protected within a database. Stored execution records can be reloaded for review. Deletion of database entries is not supported. The user must establish guidelines and procedures for the operators of the instrument to back up the database regularly.
11.10 (d) Limiting system access to authorized individuals.	SPT Labtech (Technical) User (Procedural)	A password and unique user login name is necessary for the use of the instrument. The portions of the software for the service of the instrument is password controlled at the user access level intended for SPT Labtech personnel only. Users and User groups are manged via firefly software settings. Therefore, password management, tracking of logins, login attempts must be set within the firefly software. The user has to ensure regular review of the user audit trail which must be part of the systems procedural compliance.
11.10 (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. Record 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.	SPT Labtech (Technical)	All data generated within the firefly software is stored and maintained within the database. All settings and processes are stored together with the data and tracked within an audit trail. Original Data outputs cannot be overwritten. Changes to records will not obscure previous database entries. Full username, time and type of action will be tracked in the database and made visible within the audit trail. The audit trail can be exported and printed for inspection purposes.
11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	SPT Labtech (Technical) User (Procedural)	The user group to which a user is assigned defines which parts of the software they are permitted to use. The system checks whether values entered in are in an appropriate sequence (ex: tips must be removed from the head). Scheduling of instrument performance checks must be defined by the user and must be part of the system's procedural compliance.
11.10 (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.	SPT Labtech (Technical)	The firefly software offers default user groups with different access levels based on definitions set by the designated administrator account. Configurations of the default settings are permitted at an administrator level and is the responsibility of the designated administrator account to ensure that the settings are appropriate for each user access level.
11.10 (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	SPT Labtech (Technical)	The firefly software is the only device that is able to write into the database. The user control functionality inhibits access to the database by unauthorized persons.
11.10 (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.	SPT Labtech (Technical) User (Procedural)	Reliance service engineers are trained and certified to provide install service (including IQ/OQ) and maintenance firefly Instruments. The training of the end users of the firefly instrument is the responsibility of the end user and should be part of the system's procedural compliance. SPT Labtech can provide in-house or off-site user training on the instrument and the software to provide support for this requirement.
11.10 (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.	User (Procedural)	The user has to ensure that individuals are accountable for actions undertaken under their electronic signature and must be part of the system's procedural compliance.
11.10 (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.	SPT Labtech (Technical) User (Procedural)	System and software related documentation is provided on a portable electronic data storage device (e.g. USB flash drive) delivered together with the instrument and cannot be changed. It is the responsibility of the user to maintain and provide controls and documentation of the installed system. This must be part of the system's procedural compliance. The software, printouts, and data exports contain the version information. It can also be included in the user's documentation.

Controls for Open Systems

21 CFR Part 11 Reference	Responsibility (Control)	Explanation
11.30 Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	SPT Labtech (Technical)	The firefly software itself is a closed system.
11.50 (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.	SPT Labtech (Technical) User (Procedural)	The firefly software offers the option to electronically sign protocols and results. The signer has to verify using login and password. The signing process, including a role is tracked in the audit trail and in the signed data set together with the time stamp.
11.50 (b) The items identified in paragraphs (a1), (a2), and (a3) 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).	SPT Labtech (Technical) User (Procedural)	If a signature is created, the user's name, the time stamp, and the meaning are recorded and are available for review later.
11.70 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.	SPT Labtech (Technical) User (Procedural)	If protocol or result data is signed, all details associated with this signature are tracked in its actual data set within the database and in the audit trail. It is the responsibility of the user to take action to prevent the misuse of user account names and passwords.
11.100 (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	SPT Labtech (Technical) User (Procedural)	Every signature must be created by entering full user credentials, i.e. user login and password. It is with the user's responsibility to assure by the help of firefly system settings that each username is unique and cannot be assigned to another user or re-used.
11.100 (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.	User (Procedural)	User is responsible for compliance with parts (b) to (c)
11.100 (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.	User (Procedural)	Responsibility of user.
11.200 (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. (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. (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. (2) Be used only by their genuine owners; and (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.	SPT Labtech (Technical) User (Procedural)	Every time a signature is given consists of entering full user credentials, i.e. user login and password. It is with the user's responsibility to assure by the help of firefly system a single username is restricted to a single person's use. Only this person must know the password for their username
11.200 (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable	Not applicable

Controls for Identification Codes/Passwords

21 CFR Part 11 Reference	Responsibility (Control)	Explanation
11.300 (a) Controls for identification codes/passwords. 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: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	SPT Labtech (Technical)	The firefly software enforces the requirement for a unique username and will not allow multiple accounts to be made under an identical username.
11.300 (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	SPT Labtech (Technical) User (Procedural)	Controls for password length and complexity, expiry date, number of failed log ins, and time until automatic log out when system is idle can easily be set up within the firefly software and adapted to the end user policies. Some restrictions will apply as passwords are set up to be 6-digit pin number, allowing for ease of entry using the firefly tablet.
11.300 (c) Following loss management procedures to electronically deauthorize 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.	Not applicable	Not applicable
11.300 (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 organizational management.	SPT Labtech (Technical) User (Procedural)	It is the responsibility of the end user to check the failed login reports on a regular basis to discover attempts to circumvent the security procedures.
11.300 (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.	Not applicable	Not applicable

References

1. Code of Federal Regulations, Title 21 Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter A General, Part 11 Electronic Records; Electronic Signatures. www.ecfr.gov.