DeNovix Spectrophotometer / Fluorometer

EasyApps® Secure

21 CFR Part 11 Compliance Ready Software

Applicable Models:

DS-11, DS-11+, DS-11 FX, DS-11 FX+
QFX, DS-C

Technical Note 217

21 CFR Part 11 Software Compliance Statement

DeNovix Inc.
3411 Silverside Road
Hanby Building
Wilmington, DE 19810 USA

Phone: +1.302.442.6911
Fax: +1.302.792.7407
Email: info@denovix.com
www.denovix.com

Document Control

Document #	Version	Author	Date	Description
217	A	DeNovix Inc.	April 16, 2021	First publication. For use with DS-11 software versions 4.1.0 and later.

Background

DeNovix EasyApps® Secure is an optional software suite for DeNovix Spectrophotometer / Fluorometer Products. EasyApps® Secure allows facilities to comply with the United States Food and Drug Administration Code of Federal Regulation Title 21, Part 11; Electronic Records, Electronic Signatures (21 CFR Part 11). The software provides a method of regulatory compliance; however, it is the responsibility of the end user organization and system administrators to ensure full compliance with all sections of the regulation.

How DeNovix EasyApps Secure Enables Compliance with 21 CFR Part 11

EasyApps Secure modifies the operating software so that the device functions as a closed system. Obtain an activation code from DeNovix or a DeNovix Distributor. During activation, a convenient configuration wizard guides the activating administrator through a series of steps to define the Roles, Signature Meanings, Password Rules and User accounts information. After completing activation, system access is only possible through unique User ID, password-protected accounts. Electronic signatures are enabled according to the Role assigned for each User ID. The system enables electronic signature of records for the user logged into the device. No additional PCs or tablets are required. Please see each product User Guide for detailed instructions.

In this document, each relevant 21 CFR Part 11 section and paragraph is listed. For each section, the compliance features of the DeNovix software as well as the responsibilities of the customer organization and system administrators are detailed.

IMPORTANT: In accordance with FDA regulations, DeNovix does not claim that its software or products are certified as 21 CFR Part 11 compliant. EasyApps® Secure software provides a mechanism for compliance, however the software itself does not guarantee customers are complying with Code of Federal Regulations Title 21 Part 11 - Electronic Records, Electronic Signatures. Compliance is the responsibility of the customer organization, system administrators and end users. All customer parties must abide by the requirements of the regulations to ensure complete compliance. The customer organization is solely responsible for establishing and following standard operating procedures as applicable for the facility.

21 CFR Paragraph	Compliance Details
Part 11.10 Controls for closed systems	
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. Such procedures and controls shall include the following:	DeNovix EasyApps® Secure software enables 21 CFR Mode, creating a closed system and a user interface able to comply with this regulation. Facility Standard Operating Procedures (SOPs) and the System Administrators are responsible for ensuring security measures for data handling and system access are followed.
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	IQ/OQ documentation is available for system validation purposes and to confirm the proper function of the instrument. Data is stored on the device in a format that is not directly accessible to the user. Only electronically signed records are saved on the device. Only the sample name can be modified of a signed result. This action requires a new electronic signature to save the new sample name.
(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.	Records may be exported in human readable format as a pdf file or sent to a network printer. The hash (MD5 Sum) value of a csv file containing the reported results, along with electronic signatures of each result, are included in the pdf. Audit trail details may be exported as a csv by a system administrator.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All results are stored on the system in electronic format and may be exported at any time in pdf format. The software allows signed records to be exported after each measurement session or when desired. This creates an accurate and complete copy of the result at the time of signature. DeNovix recommends that facilities establish SOPs for export of records to a secondary location that is regularly backed up according to the organization's records retentions requirements.
(d) Limiting system access to authorized individuals.	Only authorized users with a valid User ID and password can access the system.
(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.	A time-stamped audit trail is created for all signature events. Only results that are electronically signed are saved and may be exported from the system. Records may only be deleted if they have been previously exported and then are subsequently archived by a system administrator. The audit trail records all of these actions. A system administrator can search and export the audit log reports via .csv file for further inspection. Organizations should establish SOPs for routinely exporting a full copy of the audit trail database to csv in order to ensure records are available for agency review.

21 CFR Paragraph	Compliance Details
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	SOPs for proper blanking, proper measurements and creation of custom methods, assays or sample types are the responsibility of the customer.
(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.	System administrators set user access through the User Accounts app on the system. Each user has a unique ID and is assigned a Role. The user's Role establishes which Signature Meanings are permitted for the user.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	User training and SOPs for proper blanking, proper measurements and creation of custom methods, assays or sample types are the responsibility of the customer.
(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.	User training and SOPs for proper blanking, proper measurements and creation of custom methods, assays or sample types are the responsibility of the customer. The product User Guide provides detailed instructions on using the electronic record/electronic signature system within the device. The customer is responsible for training users on the proper use of EasyApps Secure software.
(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.	Responsibility of the customer and system administrators.
(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.	A release-specific User Guide is included onboard with each software release. DeNovix software releases are developed, tested and documented according to written procedures. Software updates are logged in the audit trail log. The software and firmware versions are saved as part of the sample data file. A release history is available from the DeNovix website.
11.30 Controls for open systems.	
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.	Not applicable. DeNovix instruments with EasyApps Secure operate as a closed system.

21 CFR Paragraph	Compliance Details
11.50 Signature manifestations.	
(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.	EasyApps Secure requires unique User IDs for each individual accessing the system. The system administrators manage the user accounts. (1) User ID, first name and last name as entered by the system administrators is required and included in signatures. (2) The date and time of a signature is captured and linked to the signed record. Any signature event is recorded in the Audit Trail log. (3) Each user is assigned to a Role within the organization by the system administrators. Each Role, and therefore User, can electronically sign with permitted Signature Meanings.
(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).	Any signature manifestation associated with a record may not be directly accessed or modified. All signature manifest information is saved within the system and linked to signed result record. Records may be exported in human readable format as a pdf file or sent to a network printer. The hash (MD5 Sum) value of a csv file containing the reported results, along with electronic signatures of each result, are included in the pdf.
11.70 Signature/record linking.	
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.	Any electronic signature associated with a record may not be directly accessed, deleted, transferred or modified. Each signed result includes a unique result ID that provides further confirmation of record linkage.
11.100 General requirements.	
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	A unique User ID is required for each user. Facilities and system administrators are responsible for ensuring users do not share sign-in credentials and follow compliance requirements.
(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.	Responsibility of the customer and system administrators.

21 CFR Paragraph	Compliance Details
(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.	Responsibility of the customer and system administrators.
11.200 Electronic signature components and controls.	
(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.	Users must login using their unique User ID 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.	Users login for a continuous period of controlled system access using their unique User ID / password. The User ID and password is used to sign the first record of a session. User ID is used to for subsequent signings.
(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.	Any system access for signing records requires individuals log in with User ID and password
(2) Be used only by their genuine owners; and	Responsibility of the customer and system administrators to ensure security rules are followed in the organization.
(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.	Each individual has a unique User ID and password. Customer is responsible for establishing SOPs to ensure that system administrator password resets follow organization security procedures.
b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Biometric electronic signatures are not possible with this software. This is not applicable.

21 CFR Paragraph	Compliance Details
11.300 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:	A unique User ID is required for each user. Facilities and system administrators are responsible for ensuring users follow security procedures.
(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.	EasyApps Secure requires each user to have a unique User ID.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	System administrators set password rules for the organization according to the organization's security requirements. Mechanisms for periodic password expiration and user account lockout after login failures are included in the 21 CFR App administrator controls.
(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.	System administrators can deactivate user accounts, create new accounts and issue temporary passwords for users. The customer is responsible for ensuring SOPs are established for these activities.
(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.	EasyApps Secure requires login using a unique User ID. A User ID is automatically locked (deactivated) after login failures exceed the failure limits set by the system administrators.
(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.	Users must login using their unique User ID and password. Preventing unauthorized facility or device access is the responsibility of the customer.

Disclaimer

The material in this document and referred documents is for information only and is subject to change without notice. While reasonable efforts have been made in preparation of these documents to assure their accuracy, DeNovix Inc. assumes no liability resulting from errors or omissions in these documents or from the use of the information contains herein.

DeNovix Inc. reserves the right to make changes in the product without reservation and without notification to its user.

DeNovix Inc. assumes no liability regarding the cited text from the 21 CFR Part 11 regulative and directs software users to the United States Food and Drug Administration for questions or clarifications regarding 21 CFR Part 11 regulations.