WHITE PAPER

EnVision Nexus & Kaleido Enhanced Security Software - Guide to 21 CFR Part 11 Compliance

Introduction

The EnVision® Nexus™ multimode plate reader delivers the new standard for high-throughput screening, giving you robust performance and reliable data, time after time. It operates on a brand-new innovative platform that fast tracks your research, delivering the speed and accuracy you need for your most demanding applications.

Ensuring that laboratory processes are compliant with the regulations of the U.S. Food and Drug Administration (FDA)* can be time-consuming and laborious, requiring meticulous documentation of procedures and record-keeping. A combination of software tools and administrative procedures, when well-aligned, can pave the way towards compliance.

For the EnVision Nexus, our fastest, most sensitive plate reader, the Enhanced Security option is available as an add-on to the Kaleido™ software. It provides a variety of tools to guide you towards 21 CFR Part 11 compliance. Specific reference to the relevant paragraphs of 21 CFR Part 11 is contained in this document to help you facilitate compliance with the EnVision Nexus and Kaleido software.

EnVision Nexus

*Such as 21 CFR Part 11 and other references, e.g. Annex 11 published by the European Commission

revvity

21 CFR Part 11 Reference

Subpart B – Electronic Records

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.

Responsibility: User with help from Revvity

Explanation

With the Enhanced Security software, the EnVision Nexus is a closed system. Revvity delivers support with user training. In the system, features that ensure authenticity, integrity, and confidentiality of electronic records are activated. Automated verification routines are implemented 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.

Responsibility: User with help from Revvity

Explanation

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. Revvity can deliver substantial support with user training, IQ and OQ services. The Audit Trail is provided to track alteration of 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.

Responsibility: Revvity (Technical)

Explanation

Result reports and Audit Trails can be displayed on screen and exported from the EnVision Nexus Enhanced Security software. Only user with the role "Security Administrator" can export the Audit Trail. The other roles can only view the Audit Trail.

11.10 (c)

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

Responsibility: Revvity (Technical), User (Procedural)

Explanation

All data generated with the EnVision Nexus system is stored and protected within a relational database. Stored results can be reloaded for review. The user must establish guidelines and procedures for the operators of the instrument to back up the database regularly. Certain users can delete data from the database however, these actions are documented in the Audit Trail. The Audit Trail can never be edited or deleted. The Audit Trail is part of the database backup.

11.10 (d)

Limiting system access to authorized individuals.

Responsibility: Revvity (Technical), User (Procedural)

Explanation

A password and unique user login name is necessary for the use of the instrument controlled by the Enhanced Security option. Users are managed via Windows settings. User roles are managed via the Kaleido Policy Manager. Therefore, password management, tracking of logins, login attempts, logoffs, and management of failed login attempts must be set in Windows, according to SOPs. The user must ensure regular review of the user Audit Trail which must be part of the system's 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.

Responsibility: Revvity (Technical)

Explanation

All data generated with the EnVision Nexus under control of the Kaleido Enhanced Security option is stored and maintained within the relational database. All settings, processes (such as protocol runs) and results are stored together with the data and tracked within an Audit Trail. Original data cannot be overwritten. Changes to records will not obscure previous database entries. Changes will generate a new data set. Full user name, time and type of action will be tracked in the database and made visible within the Audit Trail. The Audit Trail can be exported for inspection purposes.

11.10 (f)

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Responsibility: Revvity (Technical), User (Procedural)

Explanation

Protocols with automated data collection, and data export can be set up within the Kaleido software. The setup of the protocols is the responsibility of the user. The user role to which a user is assigned defines which parts of the software they are permitted to use. The system checks whether values entered are within acceptable range, and if accessories (e.g. filter modules) were changed and are appropriate for the selected method in a protocol to ensure the validity of the data. 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.

Responsibility: Revvity (Technical)

Explanation

The Kaleido policy manager offers default user roles with different access rights for the software. Only a Kaleido Security Administrator can edit these user roles in the Kaleido Policy Manager to adapt the access levels of the individual users to the needs within the organization. Individual roles with specific permission rights can be assigned to each authorized user of the system. The available roles are 'Security Administrator,' 'Administrator', 'Editor', and 'Operator'.

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.

Responsibility: Revvity (Technical)

Explanation

The EnVision Nexus with Kaleido software is the only device that is able to write into the relational database. The user control functionality inhibits access to the database by unauthorized persons. Only one user can be logged into the system and input can only come from logged in users.

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.

Responsibility: Revvity (Technical), User (Procedural)

Explanation

Revvity service engineers are trained and certified to provide install service (including IQ/OQ) and maintenance for Multimode Detection (MMD) instruments. The training of the end users of the EnVision Nexus instrument is the responsibility of the user and should be part of the system's procedural compliance. Revvity 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.

Responsibility: User (Procedural)

Explanation

The user must 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.

Responsibility: Revvity (Technical), User (Procedural)

Explanation

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, print-outs, and data exports contain the version information. It can also be included in the user's documentation.

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.

Responsibility: Revvity (Technical)

Explanation

The EnVision Nexus with Kaleido software itself is a closed system.

Revvity offers an option to transfer measurement data to further third party software, e.g. MyAssays® Desktop (MyAssays Ltd) for further data analysis. With the implementation of an electronic certificate, record integrity is implemented for this data transfer.

11.50 (a)

Signature manifestations. 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.

Responsibility: Revvity (Technical)

Explanation

The EnVision Nexus Kaleido Enhanced Security software offers the option to electronically sign protocols and results. The signer must verify using login and password. The signing process, including a signature role (Creator/Reviewer/Approver) is tracked in the Audit Trail and in the signed data set together with the time stamp.

11.50 (b)

Signature manifestations.

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).

Responsibility: Revvity (Technical)

User (Procedural)

Explanation

If a signature is created, the user's name, the time stamp, and the signature role are recorded and are available for review later.

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.

Responsibility: Revvity (Technical)

User (Procedural)

Explanation

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.

Subpart C – Electronic Signatures

11.100 (a)

General requirements.

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

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.

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: Revvity (Technical), User (Procedural)

Explanation

Every signature must be created by entering full user credentials, i.e. user login and password.

The system access and user administration are within the responsibility of the user.

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.

   (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.

Responsibility: Revvity (Technical)

Explanation

Every time a signature is given consists of entering full user credentials, i.e. user login and password. A single username must be restricted to a single person's use. Only this person must know the password for their username.

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

Responsibility: Revvity (Technical)

Explanation

Creating signatures in the EnVision Nexus Kaleido Enhanced Security software uses the Windows user login system. Therefore, it falls under the PC administrator's responsibilities to ensure username uniqueness, expiry date, complexity, and lockout criteria.

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

Explanation

The EnVision Nexus Enhanced Security utilizes the Policy Manager to manage access to the software. 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 set up within Windows and adapted to the individual password policies of the organization.

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.

Explanation

Not applicable.

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.

Explanation

The EnVision Nexus Enhanced Security utilizes the Policy Manager to manage access to the software. The user must ensure to track failed login attempts within the operating system. It is the responsibility of the user to check the failed login reports on a regular basis to discover attempts to circumvent the security procedures.

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.

Explanation

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 Accessed August 2023

Revvity, Inc.
940 Winter Street
Waltham, MA 02451 USA

(800) 762-4000
www.revvity.com

For a complete listing of our global offices, visit www.revvity.com