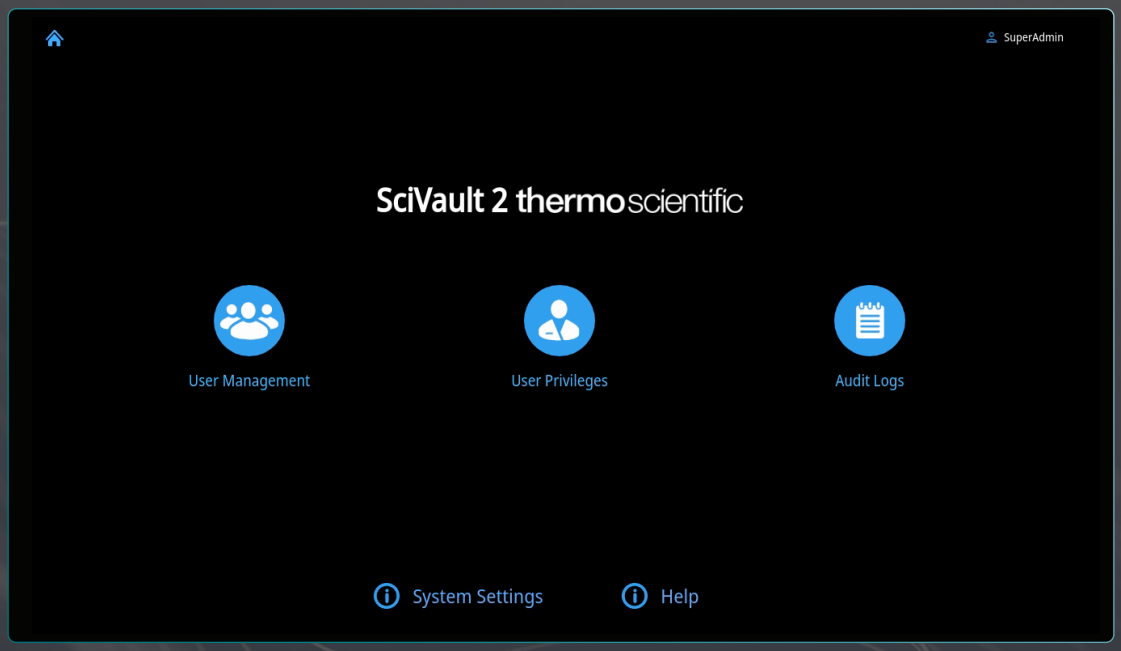



# GENESYS G5 Software & SciVault 2 Software

## Support for 21 CFR Part 11 compliance

This document explains how the Thermo Scientific™ GENESYS™ G5 Software paired with the Thermo Scientific™ SciVault™ 2 Software can help laboratories comply with the regulations in 21 CFR Part 11[1] for electronic records and electronic signatures.

[1] 21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule," Federal Register 62, no. 54 (1997): 13430-13556. World Wide Web http:/www.fda.gov.

## History

Part 11 of the 21 CFR (Title 21 – Food and Drugs of the Code of Federal Regulations) is a document issued by the United States Food and Drug Administration (FDA) that outlines the FDA criteria for accepting electronic records and signatures. The regulations in the final version of 21 CFR Part 11 became effective on August 20, 1997. All industries, companies, and organizations regulated by the FDA that utilize electronic records must follow these regulations.

In 1991, the FDA met with representatives from the pharmaceutical industry to determine how to accommodate an electronic record system, under the guidelines of current Good Manufacturing Practice (cGMP), that would create a "paperless" record system. The primary concerns of the FDA were maintaining the trustworthiness, reliability, and integrity of the electronic records and ensuring that electronic records were equivalent to paper records. The 21 CFR Part 11 regulation was created to prevent fraud in the generation and signing of electronic records.

## Definitions

Understanding the following terms is essential for the successful implementation of the regulations in 21 CFR Part 11. These definitions, taken directly from 21 CFR Part 11, will be the starting point for our discussion of Thermo Fisher Scientific's software regarding compliance with the regulation.

**Closed system**—An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

**Open system**—An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

**Digital signature (DS)**—An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

**Electronic record**—Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

**Electronic signature**—A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

**Software application template files**—Any such software files like those that may include parameter files, custom methods and kinetics methods.

## Key subparts of Part 11: Electronic records; electronic signatures

21 CFR Part 11 is divided into three subparts:

- **Subpart A** defines the scope and implementation of the regulations and defines key terms in the document.
- **Subpart B** describes requirements for electronic records, including controls for data generation from closed and open systems as well as information associated with the electronic signature and linking the signature to the record.
- **Subpart C** details the requirements, components and controls of electronic signatures.

## Software

The SciVault 2 software package is designed under the strict guidelines of Thermo Fisher Scientific's ISO 9001 certified product development process at our development and manufacturing sites in Madison, Wisconsin, and Shanghai, China. Trained members from different functional departments at our facility adhere to quality guidelines covering all aspects of development. Each software development project begins with specifications created with our customers' needs in mind. The software designs are based on object-oriented and modular architecture. Software development practices follow our Product Development Process, which includes procedures for change control, source-code control systems, and defect management. Complete user documentation is created for every project. Intensive verification and regression testing of the software is performed according to the project test plan. The qualification package can be used to verify the consistency and accuracy of the spectrophotometer's operation compared with specified limits.

## 21 CFR Part 11 compliance statement

When Scivault 2 software is activated on the Thermo Scientific™ GENESYS™ G5 instrument, the following tools will help you achieve compliance with 21 CFR Part 11 in a laboratory setting:

- System logins and passwords
- Role-based access control over software features in an easy-to-use interface
- An extensive set of software policies that allow control over program and file or data record operations
- Embedded spectral history tracking, including user information, spectrophotometer parameters, and any data manipulation information produced throughout the life of the file or data record
- Complete software use and event audit trails using a custom log, even when the software is not running
- Digital signatures with reports, data, configurations, method, and experiment files.
- Direct on-board user management or indirect user management through connection with Windows™ Active Directory
- Data record overwrite protection
- The ability to detect changes or data tampering through encrypted digital signatures
- Added data security when connecting to a LIMS by generating an API Key

When operating in a remote SciVault 2 server configuration, Windows security is embedded within the software structure and is configured through Windows security features. User authentication and access control can be managed through Windows accounts and associated security policies. Those responsible for maintaining system records must take measures to ensure the software operates within a closed system.

The following sections explain how you can use the software tools listed above to help you meet each requirement of the 21 CFR Part 11 regulation. Certain sections of the regulation are solely the responsibility of the owner of the system; we cannot directly provide tools for compliance with those specific sections. It is important to note that compliance with 21 CFR Part 11 extends beyond software implementation and will require laboratory and computer procedures that control all phases of electronic record creation and management.

**Note:** In this document, specific requirements from the 21 CFR Part 11 Electronic Records/Electronic Signature rule are shown in italics with quotation marks. Our capability to meet these requirements is shown in plain text after the statement of the requirement.

# Part 11: Electronic records; electronic signatures

This section covers Subparts B and C of 21 CFR Part 11.

## Subpart B: Electronic records

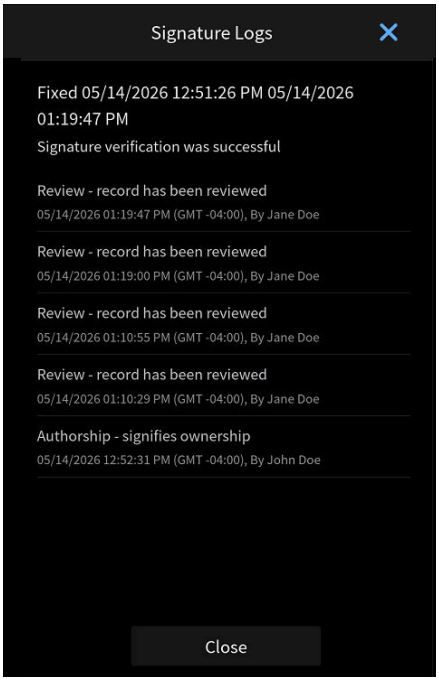
### §11.10 Controls for closed systems

*"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 repudiate the signed record as not genuine. Such procedures and controls shall include the following:*

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

The system owner must develop a protocol for validating the system. We offer a suite of products and services for the qualification of your laboratory. These offerings provide you with the tools, documentation and certification services that make system qualification efforts progress smoothly.

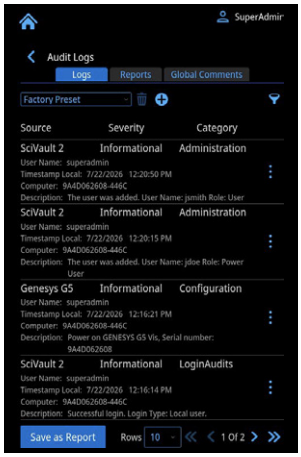
The ability to detect invalid or altered records is controlled by using the digital signature option in the software. With digital signatures, result data, application template files and audit log report files can be digitally signed, ensuring the validity of the record. By checking for the presence of a correct digital signature, the software can detect invalid or altered records.




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."*

When data is collected, detailed information about the experiment and instrument is stored in a non-editable, file-embedded spectral history. If and when the data is post-processed in any manner, details about the processing operation are noted in the data's history (Signature Logs). Information about system user and digital signatures is also stored. You can view and print the data files and their history at any time, if desired. The system owner is responsible for which format will be used to save data.

SciVault 2 software also provides a record of detailed information to be stored in a database. The database includes all data record information listed above, and data records and history can be viewed and printed at any time using the Audit Logs application.



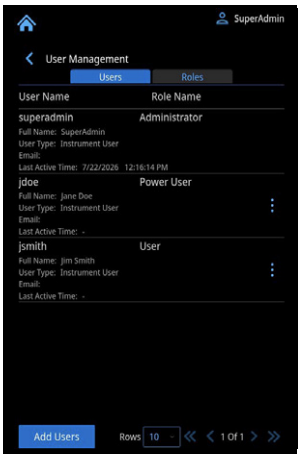

*c. "Protection of records to enable their accurate and ready retrieval throughout the records retention period."*

You can store data created by the software directly to a secure server. The system owner or IT group must determine how the files will be archived and who has access to these records. SciVault 2 software offers data storage directly to a database on a secure server. All other applications offer secure data file storage directly to a secure server.

*d. "Limiting access to authorized individuals."*

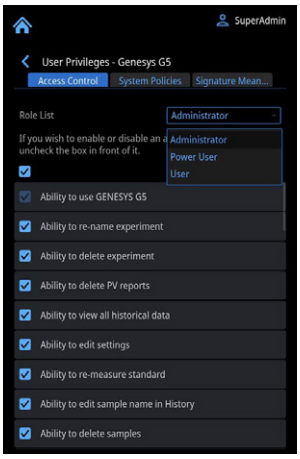
Access to the system is limited through user authentication and role-based authorization controls. When SciVault 2 software is activated on the GENESYS G5 instrument, users can be managed through locally created instrument accounts or through integration with an LDAP directory service. When operating in a remote SciVault 2 server configuration, user authentication can be managed through Windows security features and associated user account controls.

Users must be assigned unique credentials and appropriate authorization roles. The User Management and User Privileges features allow administrators to restrict access to software functions, security settings, electronic signatures, and data operations based on assigned roles. Control of file operations performed outside the software environment remains the responsibility of the system owner.




The login feature on the local instrument or on a PC through use of Windows software allows system administrators to restrict system access to only authorized users. To gain access to the software, users must log in using their username and password (when operating through a PC this would be the Windows username and password). To ensure full security, the user shall be given a unique username and a private password.

The system administrator can configure users' Roles to restrict their software access to only the programs they need. A Windows system must be configured with a secure file system in order to grant individual read, write and delete access to users. The User Privileges application is used to set access privileges to data records, features, security policies and signature meanings. Control of file operations on a computer that are conducted external to the software application is the responsibility of the system owner.




*e. "Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and action 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."*

When data is collected, detailed information about the date and time, operator, experiment, and instrument are stored in a non-editable, file- or database-embedded spectral history. (In addition to the spectral history, SciVault 2 software also stores this information in its database.) The SciVault 2 OQ is used to perform operational qualification of the SciVault 2 software.

The history provides an internal recording of all data manipulations for any given data file after it is created. Thus, SciVault 2 software will log any attempt to create, modify or delete any Thermo Fisher Scientific records on the system.

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

The software can enforce step sequencing and events for all aspects of data collection, processing and archiving. Sequenced step files can be created in the software. These files can specify and sequence the complete process: collection of parameters, data collection, final formats, post-processing operations, and archiving of data. The software can be configured so that users can access ONLY files in a specific network location.

User access privileges are managed through the SciVault 2 User Management and User Privileges features. Membership in the Administrator Role can control the extent of software access granted to each user. The system administrator or IT group must establish access failure criteria, and it is the responsibility of the Windows administrator to set these security features to ensure only authorized individuals have access to the system. If the sequence in the test data has been altered, the software notifies the user, the signature is invalidated, and the test will not run.

*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."*

The system administrator or IT group must establish access failure criteria, and it is the responsibility of the Windows administrator to set these security features to ensure that only authorized individuals have access to the system and data records on the system.

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

The system firmware and software application template files determine the validity of the input or operational instruction of the instrument. The system firmware is an IQ-qualified standard component of the instrument and can only be updated by a trained and certified Thermo Scientific service representative. Changes to the software application template files are controlled by user-access policies set up by the system administrator. Administrators can save the software application template files in a secure Windows file system to prevent unauthorized users from changing the operation parameters of the system.

*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."*

We train our system developers and maintain training records according to our internal training procedure. A training matrix is maintained along with individual training records for each developer. Thermo Fisher Scientific is ISO 9001 certified and follows these guidelines when developing all products.

Our service representatives must be trained in order to maintain and service our instruments and software. Service representatives receive training on the qualification and security software and must be recertified every two years. A training matrix is also maintained for our service representatives.

It is the responsibility of the system owner to determine that persons who develop, maintain, or use electronic record/ electronic signature systems at your site have the education, training and experience to perform their assigned task.

*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."*

To deter falsification or fraud, the system owner must establish written policies that hold individuals accountable for actions initiated under electronic signatures.

*k1. "Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance."*

The software is supplied with documentation for the operation and maintenance of the instruments and software. You can use the information in the documentation to create Standard Operating Procedures (SOPs). It is the responsibility of the system owner to control the system documentation.

*k2. "Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation."*

Our documentation contains version information that can be incorporated into the system owner's documentation control system. You can obtain information about software and firmware version numbers by choosing "About" in the Help menu. The system owner must implement a change control protocol for system 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."*

The software is intended for deployment in a closed system environment although we do employ data encryption in our database. Windows security is embedded in the software structure, and security is set up through the Windows security feature. The Windows login and password, in conjunction with the password reverification required when a user starts the software, provide a way to control access to the software and an instrument. By following the guidelines in this document, you can achieve compliance with 21 CFR Part 11 as it pertains to a closed system.

Although data encryption is used, the system administrator may choose to store the data on a secure server (recommended) such that only authorized users may access data according to their privileges. These privileges must be controlled by a unique username and password combination.

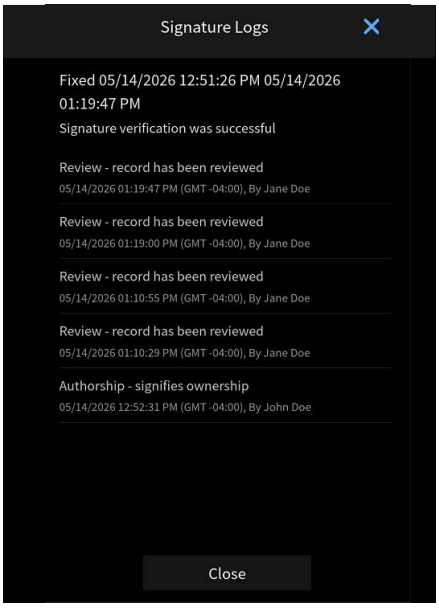
If compliance is desired in an open system, those responsible for maintaining system records must take adequate measures to ensure that the software complies.

## §11.50 Signature manifestations

*l. "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."*

All digital signatures produced by the software contain the information specified by the regulations, in addition to the signature.




*m. "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)."*

Since digital signatures implemented in the software are embedded within the electronic record, these signatures are subject to the same controls as the electronic record. The signature is included as part of the human readable and printed form of the electronic record.

## §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."*

The digital signature is stored in the same database along with the data or report that it signs. All digital signatures produced by the software are directly linked to the electronic record. A check of the electronic record can reveal an invalid electronic record.

## Subpart C: Electronic signatures

### §11.100 General requirements for electronic signatures

a. *"Each electronic signature shall be unique to one individual and shall not be reused, or reassigned, to anyone else."*

The system owner's policy for assigning local instrument user IDs passwords or Windows user IDs and passwords must comply with this requirement. This can be accomplished by assigning a unique username to each individual and by not reusing or reassigning any usernames. If the usernames are unique for all individuals with access to the system, the digital signature produced by the software will be unique.

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

The system owner must take appropriate measures to ensure the identity of all individuals who may be involved in applying electronic signatures to records.

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."*

In order to have an electronic signature, the organization using the signature must make it legally binding by submitting a letter and a form to the FDA.

### §11.200 Electronic signature components and controls

a. *"Electronic signatures not based upon biometrics shall:*

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

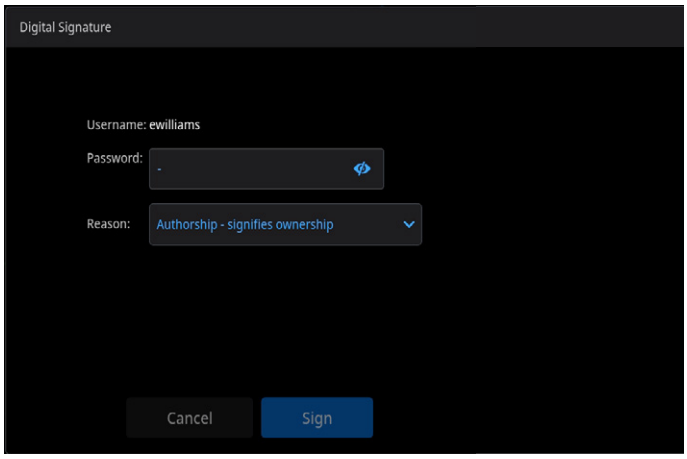
      i. *When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable 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 owner; 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."*

Digital signatures used by the software are based on the user's login ID and their own password. Our software is used to generate the digital signature in the system, and the combination of the signature components is unique for each user, as long as the requirements in 11.100 (a) are met. All signings in the software require entering the password of the person who is logged in to the Windows session or local instrument control software at the time of system use. The system owner and administration must implement a protocol for using electronic signatures as described in requirements (2) and (3) are met.




b. *"Electronic signatures based on biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners."*

This requirement does not apply to our software because we use digital signatures based on the combination of a username and password, instead of biometrics.

### §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."*

The system administrator or IT group must ensure that the combination of ID code and password is unique for each individual. This can be easily accomplished by issuing each user a unique login identification.

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

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.*

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."*

Windows security features simplify the process of periodic checking, recalling and revising of log-ins and passwords. Transaction safeguards to prevent unauthorized access to the system are also available in the Windows operating system.

Limiting the number of failed login attempts and creating a password for an aging procedure is a common safeguard to limit and log the number of failed login attempts. Consult your Windows documentation for more information about activating system safeguards. The system administrator must establish a procedure for checking ID codes and passwords and loss management.

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."*

Because our software does not use cards or tokens to generate identification codes, this requirement does not apply.

## Summary

This document was created based on Thermo Fisher Scientific's interpretation of the regulations and through consultation with experts in the field. The software with the digital signature option can be used together with proper procedures and controls instituted by our customers, in accordance with an FDA compliant process.

## More about 21 CFR Part 11

For more information about the requirements of 21 CFR Part 11, go to **fda.gov**

We are dedicated to working with our customers to help meet their regulatory needs wherever possible. For more information contact **thermofisher.com**

**For research use only. Not for use in diagnostic procedures. For current certifications, visit thermofisher.com/certifications**
© 2025-2026 Thermo Fisher Scientific Inc. All rights reserved. Microsoft and Windows are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of Thermo Fisher Scientific Inc. and its subsidiaries. **MCS-TN1949-EN 9/26**