

VISION_{security} Software:
21 CFR Part 11 Compliance



The information in this publication is provided for reference only. All information contained in this publication is believed to be correct and complete. Thermo Fisher Scientific shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this material. All product specifications, as well as the information contained in this publication, are subject to change without notice.

This publication may contain or reference information and products protected by copyrights or patents and does not convey any license under our patent rights, nor the rights of others. We do not assume any liability arising out of any infringements of patents or other rights of third parties.

We make no warranty of any kind with regard to this material, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Customers are ultimately responsible for validation of their systems.

© 2006-2007 Thermo Fisher Scientific Inc. All rights reserved. Microsoft, Windows and Windows NT 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. No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photograph, magnetic or other record, without our prior written permission.

For technical assistance, please contact:

Technical Support
Thermo Fisher Scientific
5225 Verona Road
Madison WI 53711-4495
U.S.A.

Telephone: 1 800 642 6538 (U.S.A.) or +1 608 273 5017 (worldwide)

Fax: +1 608 273 5045 (worldwide)

E-mail: us.techsupport.analyze@thermofisher.com

World Wide Web: <http://www.thermo.com/spectroscopy>

269-192100, rev.A

Contents

VISION<i>security</i> Software: 21 CFR Part 11 Compliance	1
History.....	1
Definitions.....	2
Key subparts of Part 11: Electronic records; Electronic signatures	3
VISION <i>security</i> software	3
21 CFR Part 11 Compliance Statement	4
Part 11: Electronic records; Electronic signatures	6
Subpart B: Electronic records.....	6
§11.10 Controls for closed systems	6
§11.30 Controls for open systems.....	12
§11.50 Signature manifestations	13
§11.70 Signature/record linking	13
Subpart C: Electronic signatures	14
§11.100 General requirements for electronic signatures	14
§11.200 Electronic signature components and controls	15
§11.300 Controls for identification codes/passwords	16
Summary	17
More about 21 CFR Part 11	18
Questions or concerns.....	18

VISION*security* Software: 21 CFR Part 11 Compliance

This document explains how Thermo Scientific's VISION*security*[™] software can help you comply with the regulations in 21 CFR Part 11 for electronic records and electronic signatures.

Note VISION*security* is available for the Windows[®] XP Professional and Windows 2000 operating systems. Unless stated otherwise, all further references in this manual to “Windows” should be interpreted as meaning either of these versions. ▲

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.

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), which 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 regulations were created to prevent fraud in the generation and signing of electronic records. This document explains how Thermo Electron's VISION*security* software facilitates compliance with the regulations in 21 CFR Part 11.

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 11¹, will be the starting point for our discussion of VISION*security*'s compliance with the regulation. This document pertains to Thermo Electron's VISION*security* software suite.

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.

Digital signature – 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.

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.

¹ "21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule," Federal Register 62, no. 54 (1997): 13430-13446. World Wide Web <http://www.fda.gov>. Accessed 20 June 2006.

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. Requirements for electronic records are described in Subpart B, 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.

VISION*security* software

This document refers specifically to VISION*security*. (The minimum recommended version is 3.0. Earlier versions do not provide a completely secure environment that supports the 21 CFR Part 11 requirements.) Every VISION*security* software package is designed under the strict guidelines of the ISO 9001 certified product development process at our development and manufacturing site in Madison, Wisconsin. 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 UV Validator Qualification package can be used to verify the consistency and accuracy of the spectrophotometer's operation within the specified limits.

21 CFR Part 11 Compliance Statement

When *VISIONsecurity* is installed, it provides the following tools to help you achieve compliance with 21 CFR Part 11 in a laboratory setting:

- System log-ins and passwords.
- Complete access control over *VISIONsecurity* software features in an easy-to-use interface.
- An extensive set of *VISIONsecurity* software policies that allow control over program and file operations.
- File-embedded spectral history tracking, including user information, spectrophotometer parameters and any data manipulation information produced throughout the life of the file.
- Complete software use and file event audit trails using a custom log in the Windows Event Viewer application, even when *VISIONsecurity* software is not running.
- Digital signatures with results and method files.
- Network and local security with Windows.
- File overwrite protection.
- The ability to detect changes or data tampering through encrypted digital signatures.

Windows security is embedded in the *VISIONsecurity* software structure and is set up through the Windows security features. You can control access to a spectrophotometer by using those features in conjunction with *VISIONsecurity* access privileges. The Windows log-in and password are used to authenticate users when an electronic record is created. Those responsible for maintaining system records must take measures to ensure that *VISIONsecurity* operates in 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 is a state that 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. 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. Certain relevant definitions in this document are taken from Subpart A. Other than this, Subpart A is not covered in this document.

Subpart B: Electronic records

This section covers Subpart B of 21 CFR Part 11.

§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 their UV-Visible spectrophotometers. These offerings provide our customers the tools, documentation and certification services that make system qualification progress smoothly. More details on our validation and qualification products and services are available upon request.

The ability to detect invalid or altered records is controlled by using the digital signature feature in VISION*security*. With digital signatures, result data, VISION*security* application method files, qualification test files, VISION*security* sample method files, accessory methods and calibration files can be digitally signed, ensuring the validity of the record. By checking for the presence of a correct digital signature, VISION*security* 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.

When spectral data is collected by VISION^{security}, detailed information about the experiment, instrument and accessory 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 history. Information about system user and digital signatures is also stored. You can view and print the spectral data files and their history at any time, if desired. The VISION^{security} software also has the ability to export experiment data into the standard .csv and .txt file formats.

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

You can store data created by VISION^{security} directly to a secure server such as a Windows system. The system owner or MIS/IT group must determine how the files will be archived and backed up and who has access to these records. It is also necessary to have a procedure to ensure that retrieval records can be read.

(d) Limiting access to authorized individuals.

Using Windows secure log-ins is required for controlling access to the system. VISION^{security} must be installed on computers that have the Windows operating system, which ensures that you can control access to the system. Windows users and groups can be configured to have access to VISION^{security} software through our Security Administration program.

The log-in feature of Windows allows system administrators to restrict system access to those who are authorized. To gain access to VISION^{security}, users must log in to Windows with their user name and password and then re-enter their Windows password when launching VISION^{security}. To ensure full security, the user should be given a unique user name and a private password. (The passwords created under Windows are encrypted using the cryptographic services in Windows. For more information, please consult your Windows documentation.)

The system administrator can configure users' profiles to restrict their software access to only the programs they need. A Windows system must be configured with a secure file system, such as NTFS, in order to grant individual read, write and delete access to users. The Security Administration software is used to set access privileges to VISIONsecurity menus, data collection and data manipulation, security policies, and signature meanings. This software should be configured so that only the system administrator or responsible personnel have access.

The Security Administration server can be installed on the local workstation or as a client-server application. Typically this software is installed on a network server to provide centralized administration for all user accounts on the network. This eliminates the need to configure many individual (client) computers.

The Thermo Log Service installed with the Security Administration software logs program use and file events for files associate with VISIONsecurity, even if VISIONsecurity is not running. These events are logged into the Windows Event Viewer in a custom log. However, for maximum security of these files external to VISIONsecurity (that is, when VISIONsecurity is not in use), we recommend that folder security be configured so that VISIONsecurity's internal files cannot be deleted. In particular, the paths specified by VISIONsecurity should be protected from file deletion. Control of file operations on the computer that are conducted external to the VISIONsecurity 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 spectral data is collected by VISIONsecurity, detailed information about the date and time, operator, experiment, instrument and accessory is stored in a non-editable, file-embedded spectral history. Whenever the data is changed and saved, detailed information about the data processing function performed, the user name and the digital signature are automatically appended to the spectral history, which preserves all of the previously stored information. VISIONsecurity also includes file overwrite protection that you can use to prevent the unauthorized or accidental deletion of data by re-saving over it. You can view and print spectral data files and their histories at any time. Since this information is embedded in the data files, it travels with the data file if it is moved or copied.

The audit trail provides an internal history of all data manipulations for any given data file after it is created using VISIONsecurity. In addition to this tool, the Thermo Log Service uses the Event Viewer of Windows as an external file operation audit trail. The Thermo Log Service uses the Event Viewer to log all file operations, both within and outside of the VISIONsecurity application even if VISIONsecurity is not running. Thus, the Event Viewer will log any attempt to create, modify or delete any records on the system, even if VISIONsecurity is not running. The system owner must establish a procedure for maintaining the audit trail log.

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

VISIONsecurity can enforce step sequencing through the Performance Verification (PV) tests through automating the Calibration Verification Carousel (CVC). These files are stored with extension format *.vre.

Each PV test results file generated using VISIONsecurity during Operational Qualification can be electronically signed. Test results files contain the sequence of events for the qualification tests performed. These files contain the serial number of the instrument, the serial number of the CVC, the date and time of the test, the tolerances of the standards used to perform the tests, and the status of the applicable lamp(s) used during the test. Electronic signatures can be forced for each PV test results file.

(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.

Because Windows security is embedded in the VISION*security* software, the user access privilege requirements and individuality features of Windows can be used. The system administrator or MIS/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 files on the system. The operator must enter his or her Windows password a second time to gain access to the VISION*security* software. In addition, security settings established using the Security Administration software (which define the user interface and control feature access) are tied to Windows user groups. Membership in a system group can then control the extent of software access a user has, including accessing the VISION*security* application itself or restricting users from accessing the Windows desktop when they are running VISION*security*.

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

Checks to determine the validity of input or operational instructions to VISION*security*, and spectrophotometers controlled by VISION*security*, are restricted and controlled by VISION*security* method files and preprogrammed command controls through system firmware. Administrators can specify and control unique experiment parameters (method files). When administrators and users select method parameters, the allowed input values for the fields are controlled by VISION*security*. Administrators can save the method files in a secure Windows file system to prevent unauthorized users from changing the operational parameters of the system.

Use of VISION*security*'s Smart Accessory™ recognition and automated spectrophotometer status checking will ensure that allowable configuration and system components are optimized for a particular experiment. The results of VISION*security*'s spectral quality checks are recorded in a non-editable file for later review and reference.

(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.

Optional training on VISION^{security} software and our UV-Visible spectrophotometers is available. This offering can assist you in training those individuals who maintain or use electronic record systems supplied by us.

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. We are ISO 9001 certified and follow these guidelines when developing all products.

Our Field Service Engineers must be trained in order to maintain and service our spectrophotometers and software. Service Engineers receive training on VISION^{security} software and the UV Validator and must be recertified every two years. A training matrix is also maintained for our Service Engineers.

(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 on-line and printed manuals for the operation and maintenance of our spectrophotometers and VISION^{security} software. You can use the information in the manuals to create 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.

Software, firmware, on-line, and printed documentation contain 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 from the Help menu of VISIONsecurity. 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 VISIONsecurity implementation requires the use of a closed system since we do not employ data encryption on our data files. Windows security is embedded in the VISIONsecurity software structure, and security is set up through the Windows security feature. The Windows log-in and password, in conjunction with the password re-verification required when a user starts VISIONsecurity, provide a way to control access to the VISIONsecurity software and a spectrophotometer. 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 not 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 user name and password combination.

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

§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.*

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

- (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).*

Since digital signatures implemented in VISIONsecurity 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 data file or report that is signed. Because the signature is stored in the same file as the electronic record, all digital signatures produced in VISIONsecurity are directly linked to the electronic record. A check of an electronic record can verify whether the signature is valid. An invalid signature could be caused by a record that was never signed or a record that was modified after it was signed. If an invalid signature was attached to an electronic record, or if the record was tampered with, simply checking the signature on the electronic file will reveal the problem.

Subpart C: Electronic signatures

This section covers Subpart C of 21 CFR Part 11.

§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 Windows user IDs and passwords must comply with this requirement, which can be accomplished by assigning a unique user name to each individual and by not reusing or reassigning any user names. If the user names are unique for all individuals with access to the system, the digital signature produced by VISIONsecurity 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 VISIONsecurity are based on the user's log-in ID and Windows password. The cryptographic service in Windows is used to generate the digital signature in VISIONsecurity, 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 VISIONsecurity software require entering the password of the person who is logged in to the Windows session at the time of system use. The system owner and administration must implement a protocol for using electronic signatures that ensures that 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 VISIONsecurity because VISIONsecurity uses digital signatures based on the combination of a user name 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 MIS/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 log-in identification.

It is not technically possible to assign more than one user to a user name if user names are not reused and are unique for every individual. Therefore, the technology enforces this solution upon the user; that is, no one, not even the system administrator, can defeat this safeguard.

(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 Windows.

A commonly implemented feature is to limit and log the number of failed log-in attempts and to set up a password aging procedure. Consult your Windows documentation for more information on checking identification codes and passwords and 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 VISIONsecurity does not use cards or tokens to generate identification codes, this requirement does not apply.

Summary

This document has been created based on our interpretation of the regulations and through consultation with experts in the field. The VISIONsecurity software 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 www.fda.gov.

We are dedicated to working with its customers to help meet their regulatory needs wherever possible. For more information:

Thermo Fisher Scientific Headquarters – United States

81 Wyman Street
PO Box 9046
Waltham, MA 02454-9046

TEL: 781-622-1006
FAX: 781-622-1207

Madison, Wisconsin

5225 Verona Road
Madison, WI 53711-4495

Questions or concerns

In case of emergency, follow the procedures established by your facility. If you have questions or concerns about safety or need assistance with operation, repairs or replacement parts, you can contact your sales or service representative in your area or use the information at the beginning of this document to contact us