



OMNIC Software: 21 CFR Part 11 Compliance

Copyright © 2005 by Thermo Electron Corporation, Madison WI 53711.
Printed in the United States of America. All world rights reserved.

The information in this publication is provided for reference only. All information contained in this publication is believed to be correct and complete. Thermo Electron Corporation 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. Thermo Electron Corporation does not assume any liability arising out of any infringements of patents or other rights of third parties.

Thermo Electron Corporation makes 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.

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 the prior written permission of Thermo Electron Corporation.

For technical assistance, please contact:

Technical Support
Thermo Electron Corporation
5225 Verona Road
Madison WI 53711-4495
U.S.A.

Telephone: 1 800 642 6538 (U.S.A.) or +1 608 276 6373 (worldwide)
Fax: +1 608 273 5045 (worldwide)
E-mail: techsupport.analyze@thermo.com

OMNIC, ValPro, and Smart Accessory are trademarks of Thermo Electron Scientific Instruments Corporation, a subsidiary of Thermo Electron Corporation.

Windows is either a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries.

269-114904



Contents

OMNIC Software: 21 CFR Part 11 Compliance	1
History	1
Definitions	2
Key subparts of Part 11: Electronic records; Electronic signatures	3
OMNIC software	3
21 CFR Part 11 Compliance Statement	4
Part 11: Electronic records; Electronic signatures.....	5
Subpart B: Electronic records.....	5
§11.30 Controls for open systems	10
§11.50 Signature manifestations.....	11
§11.70 Signature/record linking	12
Subpart C: Electronic signatures	12
§11.100 General requirements for electronic signatures	12
§11.200 Electronic signature components and controls	13
§11.300 Controls for identification codes/passwords.....	14
Summary.....	15
More About 21 CFR Part 11.....	17



OMNIC Software: 21 CFR Part 11 Compliance

This document explains how Thermo Electron's OMNIC™ Versions 6.2 and 7.0 (or higher) software can help you comply with the regulations in 21 CFR Part 11 for electronic records and electronic signatures.

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. This document explains how Thermo Electron's OMNIC software with the DS option 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 OMNIC's compliance with the regulation. This document pertains to Thermo Electron's OMNIC 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>.

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.

OMNIC software

Important This document refers specifically to OMNIC Versions 6.2 and 7.0 (or higher) with the DS data security and integrity software option installed. The DS option enables the OMNIC tools and options described in this document that will assist your compliance with 21 CFR Part 11. All references to OMNIC in this document should be interpreted as OMNIC Version 6.2 or 7.0 (or higher) with the DS option installed. OMNIC with DS is available only for the Windows® 2000 and Windows XP Professional operating systems. (All further references in this manual to Windows XP should be interpreted as Windows XP Professional.) Versions of OMNIC that do not have the DS option installed will require a hybrid record system to achieve compliance with 21 CFR Part 11 and are not covered by this document. ▲

Every OMNIC software package is designed under the strict guidelines of Thermo Electron's 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. ValPro Qualification software can be used to verify the consistency and accuracy of the spectrometer's operation compared with specified limits.

21 CFR Part 11 Compliance Statement

When the DS option is installed, OMNIC includes 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 OMNIC software features in an easy to use interface.
- An extensive set of OMNIC software policies that allow control over program and file operations.
- File-embedded spectral history tracking, including user information, spectrometer parameters and any data manipulation information produced throughout the life of the file.
- Complete software use and file event audit trails using a custom Thermo Electron log in the Windows Event Viewer application, even when OMNIC software is not running.
- Digital signatures with reports, data, macros, configurations and experiment files.
- Network and local security with Windows 2000 or Windows XP
- File overwrite protection.
- The ability to detect changes or data tampering through encrypted digital signatures.

Windows 2000 or Windows XP security is embedded in the OMNIC software structure and is set up through either the Windows 2000 or Windows XP security features. You can control access to a spectrometer by using those features in conjunction with OMNIC access privileges. The Windows 2000 or Windows XP 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 OMNIC 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; Thermo Electron 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 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. (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

§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. Thermo Electron offers a suite of products and services for the qualification of their laboratory FT-IR and Raman spectrometers. These offerings provide our customers the tools, documentation and certification services that make system qualification efforts progress smoothly. More details on Thermo Electron’s 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 OMNIC. With digital signatures, spectral data (*.SPA and *.JDX), OMNIC parameter sets, macros (*.MAC), OMNIC electronic reports, quant method files, qualification test files, and OMNIC user configuration files can be digitally signed, ensuring the validity of the record. By checking for the presence of a correct digital signature, OMNIC 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 OMNIC, detailed information about the experiment, instrument and accessory is stored in a non-editable, file-embedded spectral history. If and when the spectrum is post-processed in any manner, details about the processing operation are noted in the spectrum’s 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 OMNIC software also has the ability to save spectral data into the standard JCAMP-DX or CSV file formats, using the header conventions of those standards. The system owner is responsible for deciding how records will be maintained and which format will be used to save spectral data.

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

You can store spectral data created by OMNIC directly to a secure server such as a Windows 2000 or Windows XP 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. Besides individual spectrum files (*.SPA,*.JDX, and *.CSV), OMNIC spectral data can also be saved in OMNIC report notebooks (*.NBK). OMNIC’s report notebook feature organizes and archives experiments and measurements made by Thermo Electron spectrometers using OMNIC software. Nothing can be deleted from an OMNIC report notebook; thus it can be used to create a complete and accurate trail of all changes to spectral data. Store OMNIC report notebooks in a secure directory where the *.NBK file itself cannot be deleted. All entries into the report notebook are non-editable and are archived for future review.

- (d) *“Limiting access to authorized individuals.”*

Using Windows 2000 or Windows XP secure log-ins is required for controlling access to the system. OMNIC with the DS option must be installed on computers that have the Windows 2000 or Windows XP operating system, which ensures that you can control access to the system. Windows 2000 and Windows XP users and groups can be configured to have access to OMNIC software through the Thermo Electron Security Administration program.

The log-in feature of Windows 2000 or Windows XP allows system administrators to restrict system access to those who are authorized. To gain access to OMNIC, users must log in to Windows 2000 or Windows XP with their user name and password and then re-enter their Windows password when launching OMNIC. 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 2000 or Windows XP documentation.)

The system administrator can configure users' profiles to restrict their software access to only the programs they need. A Windows 2000 or Windows XP 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 Thermo Electron Security Administration software is used to set access privileges to OMNIC menus, data collection and search parameters, security policies, and signature meanings. This software should be configured so that only the system administrator or responsible personnel have access. The Thermo Electron Security Administration server can be installed on the local workstation or as a client-server application. The Thermo Log Service installed with the Thermo Electron Security Administration software logs program use and file events for files associate with OMNIC, even if OMNIC is not running. These events are logged into the Windows Event Viewer in a Thermo Electron custom log. However, for maximum security of these files external to OMNIC (that is, when OMNIC is not in use), we recommend that folder security be configured so that OMNIC's internal files cannot be deleted. In particular, the paths specified by OMNIC should be protected from file deletion. Control of file operations on the computer that are conducted external to the OMNIC 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 OMNIC, 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. OMNIC 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 spectral history provides an internal history of all data manipulations for any given data file after it is created using OMNIC. In addition to this tool, the Thermo Log Service uses the Event Viewer of Windows 2000 or Windows XP 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 OMNIC application even if OMNIC is not running. Thus, the Event Viewer will log any attempt to create, modify or delete any records on the system, even if OMNIC is not running. The system owner must establish a procedure for maintaining the audit trail log.

You can save spectral data and other administrator-specified information in an OMNIC report notebook as an alternative to saving spectral data as *.SPA files. The OMNIC report notebook approach to saving OMNIC data provides complete archiving of spectral data files (including all spectral header audit trails previously mentioned), date and time stamps, and log-in names and satisfies requirements for long-term archiving of spectral data.

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

OMNIC can enforce step sequencing and events for all aspects of data collection, processing and archiving. Sequenced steps (*.MAC) files can be created in the OMNIC Macros\Basic software. *.MAC files can specify and sequence the complete process: collection of parameters, data collection, final formats, post-processing operations, and archiving of data. OMNIC can be configured so that users can access only specific *.MAC files.

Each test file used by ValPro Qualification during Operational Qualification is signed at the Thermo Electron factory. The signature is verified when the software is run. Test files contain the sequence of events for the qualification. If the sequence in a test file 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.”*

Because Windows 2000 or Windows XP security is embedded in the OMNIC software, the user access privilege requirements and individuality features of Windows 2000 or Windows XP 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 2000 or Windows XP password a second time to gain access to the OMNIC software. In addition, security settings established using the Thermo Electron Security Administration software (which define the user interface and control feature access) are tied to Windows 2000 or Windows XP user groups. Membership in a system group can then control the extent of software access a user has, including accessing the OMNIC application itself or restricting users from accessing the Windows desktop when they are running OMNIC.

- (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 OMNIC, and spectrometers controlled by OMNIC, are restricted and controlled by OMNIC experiment files (*.EXP) and preprogrammed command controls through system firmware. System firmware is an initial configuration component of the spectrometer system, initially IQ-qualified, and can be updated only by a trained and certified Thermo Electron Service Engineer. Administrators can specify and control unique experiment parameters (*.EXP files) and assign OMNIC macros (*.MAC files) for sequenced stepped operations, as explained in the suggested implementation of 21 CFR Part 11, Subpart B, 11.10(f). When administrators and users select experiment parameters, the allowed input values for the fields are controlled by OMNIC. Administrators can save the experiment files in a secure Windows file system to prevent unauthorized users from changing the operational parameters of the system.

Use of OMNIC’s Smart Accessory recognition and automated spectrometer status checking will ensure that allowable optical configuration and system components are optimized for a particular experiment. The results of OMNIC’s spectral quality checks are recorded in the non-editable spectrum header 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.”*

Training classes on OMNIC software and Thermo Electron spectrometers are available from Thermo Electron at our Madison, Wisconsin site, at the Thermo Electron training facility in West Palm Beach, Florida, and at your site. These courses are available to assist you in training those individuals who maintain or use electronic record systems supplied by Thermo Electron.

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 Electron is ISO 9001 certified and follows these guidelines when developing all products.

Thermo Electron Field Service Engineers must be trained in order to maintain and service Thermo Electron spectrometers and software. Service Engineers receive training on the ValPro Qualification and OMNIC DS software and must be recertified every two years. A training matrix is also maintained for Thermo Electron 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 the Thermo Electron spectrometers and OMNIC 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 OMNIC. 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 OMNIC DS implementation requires the use of a closed system since we do not employ data encryption on our data files. Windows 2000 and Windows XP security is embedded in the OMNIC software structure, and security is set up through the Windows 2000 or Windows XP security feature. The Windows log-in and password, in conjunction with the password reverification required when a user starts OMNIC, provide a way to control access to the OMNIC software and a spectrometer. 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 OMNIC 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 OMNIC 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 OMNIC 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 OMNIC 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

§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 2000 and Windows XP 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 OMNIC 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 OMNIC are based on the user's log-in ID and Windows 2000 or Windows XP password. The cryptographic service in Windows is used to generate the digital signature in OMNIC, 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 OMNIC 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 OMNIC because OMNIC 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. 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 2000 or Windows XP 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 2000 and Windows XP.

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 2000 or Windows XP 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 OMNIC does not use cards or tokens to generate identification codes, this requirement does not apply.

Summary

This document has been created based on Thermo Electron's interpretation of the regulations and through consultation with experts in the field. The OMNIC software with the DS option can be used together with proper procedures and controls instituted by the 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.

Thermo Electron is dedicated to working with its customers to help meet their regulatory needs wherever possible. For more information contact:

Thermo Electron Headquarters – United States

Thermo Electron Corporation
81 Wyman Street
PO Box 9046
Waltham, MA 02454-9046
TEL: 781-622-1006
FAX: 781-622-1207

Madison, Wisconsin

Thermo Electron Corporation
5225 Verona Road
Madison, WI 53711-4495

To ask technical questions or receive information regarding any Thermo Electron products, please contact Thermo Electron at 800-642-6538 or techsupport.analyze@thermo.com.