

RESULT 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 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. Customers are ultimately responsible for validation of their systems. 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 the patent rights of Thermo Electron Corporation, 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.

Copyright © 2004 by Thermo Electron Corporation, Madison WI 53711. Printed in the United States of America. All world rights reserved. 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 contact:

Technical Support
Thermo Electron Corporation
5225 Verona Road
Madison WI 53711-4495

Telephone: 1-800-642-6538 (U.S.A.) or +608-273-5015 (worldwide)
Fax: +608-273-5045 (worldwide)
E-mail: techsupport.analyze@thermo.com

Nicolet, Antaris, RESULT, ValPro and TQ Analyst are trademarks of Thermo Electron Scientific Instruments Corporation, a subsidiary of Thermo Electron Corporation.
Microsoft, Windows and Windows NT are registered trademarks of the Microsoft Corporation.
Adobe and Acrobat are registered trademarks of Adobe Systems Inc.

269-115501



Contents

About RESULT™ Software	1
Understanding 21 CFR Part 11	3
History.....	3
Key subparts.....	3
Key definitions.....	4
Using RESULT to Meet 21 CFR Part 11	
Requirements.....	5
21 CFR Part 11: Electronic Records; Electronic	
Signatures.....	5
Subpart B: Electronic Records.....	5
Subpart C: Electronic Signatures	14
Summary	18
For More Information	19
RESULT Software 21 CFR Part 11 Compliance	
Document Disclaimer.....	21



About RESULT™ Software

Thermo Electron Corporation instruments use the RESULT™ software platform, which has two distinct applications: RESULT Integration and RESULT Operation. RESULT Integration is used by a lab manager, or some other trained individual, to create workflows. A workflow is a series of tasks (such as collecting data and archiving records) that are required to analyze a sample, generate a report, and archive the results. In the Integration application, the creator of the workflow specifies all collection parameters, determines which electronic records will be stored, and decides if and when digital signatures will be used.

Once a workflow has been developed so that it meets the requirements of the system owner, it is implemented in RESULT Operation, which is the application used by operators to qualify the system and run routine samples in a production environment. Based on the steps in the workflow, the operator is guided through the sample analysis and can be assigned different privileges based on his or her access level.

RESULT was designed using Thermo Electron's Madison, Wisconsin development and manufacturing site's ISO 9001 certified product development procedures. It is thoroughly documented and tested to help you meet the 21 CFR Part 11 requirements and includes the following tools:

- System log-ins and passwords
- Automatic audit trail generation
- Digital signatures with reports and data
- Electronic Standard Operating Procedures (SOPs)
- Network security with Windows®
- Report file format viewable with web browsers
- Signing and Security of TQ Analyst™ quantitative and qualitative methods
- Tamper proof reports and data files

Windows security is embedded in the RESULT software structure and is set up through the Windows security feature. The Windows logon and password are used to authenticate users when an electronic record is created, so, in conjunction with RESULT access privileges, the logon and password allow you to control access to an analyzer. Those responsible for maintaining system records must take measures to ensure that RESULT operates in a closed system. (Additional information on the system requirements and specifications for RESULT software can be found in the Thermo Electron Corporation's ValPro™ System Qualification manual.)



Understanding 21 CFR Part 11

The Electronic Signatures and Electronic Records Rule (21 CFR Part 11) outlines the FDA criteria for accepting electronic records and signatures. The FDA regulation provides companies with specific requirements for maintaining the trustworthiness, reliability, and integrity of electronic records and ensuring that electronic records are equivalent to paper records. The rule became effective on August 20, 1997 for all industries, companies, and organizations regulated by the FDA. This document explains how Thermo Electron's RESULT software can help companies ensure compliance with the regulations in 21 CFR Part 11.

History

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 21 CFR Part 11 was created to prevent fraud in the generation and signing of electronic records.

Key subparts

The 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 the requirements for electronic records, including information associated with the electronic signature, the controls for data generation from closed and open systems, and information about linking the electronic signature to the record.

Subpart C details the requirements, components, and controls for electronic signatures

Key definitions

The following definitions are taken directly from the 21 CFR, Part 11, Section 11.3 (b):

Electronic record means 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 means 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 means 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.

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

RESULT software is designed to provide electronic and digital signatures, and electronic records using non-biometric controls within a closed system.



Using RESULT to Meet 21 CFR Part 11 Requirements

This section provides the text of each requirement of 21 CFR 11, Subparts B and C in italics, followed by information on how RESULT software can be used to meet the requirement. RESULT alone cannot meet the requirements. The software contains the tools needed to demonstrate to the FDA that electronic records and electronic signatures can be generated according to regulations.

21 CFR Part 11: Electronic Records; Electronic Signatures

The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

Note There are certain sections of the 21 CFR Part 11 that are solely the responsibility of the owner of the system, and as such, Thermo Electron cannot directly demonstrate compliance with these requirements. ▲

Subpart B: Electronic Records

Subpart B of 21 CFR 11 documents the regulations pertaining to the generation and use of 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 readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

- §11.10(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. RESULT, when used in combination with Thermo Electron's ValPro System Qualification software, provides the tools you need to qualify your system and includes materials to help you meet the requirements of Design Qualification (DQ), Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ). For more information, contact your Thermo Electron representative or consult the ValPro manual or Pre-Installation Qualification Overview.

The ability to detect invalid or altered records is controlled by using the digital signature feature in RESULT. With digital signatures, all reports, data, SOPs, and other electronic records can be digitally signed, which ensures the validity of the record. By checking for the presence of a correct digital signature, RESULT can detect invalid or altered records.

- §11.10(b) *The ability to generate accurate and complete copies of records in 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 creating workflows in RESULT Integration, spectral data files can be saved in one of the following formats: Comma Separated Value (CSV), Nicolet™ Spectral Data (*.spa), Galactic (.spc), or JCAMP. Spectral files can be copied into other applications, such as MS Word or Excel, and can be viewed and printed using Thermo Electron's RESULT software or TQ Analyst package. The Nicolet Spectral Data (*.spa) format, however, is the only one that supports digital signatures. All reports created by RESULT are in HTML (Hypertext Markup Language) and can be viewed and printed using RESULT or most web browsers. (The system owner is responsible for deciding how records will be maintained and which format will be used to save spectral data.)

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

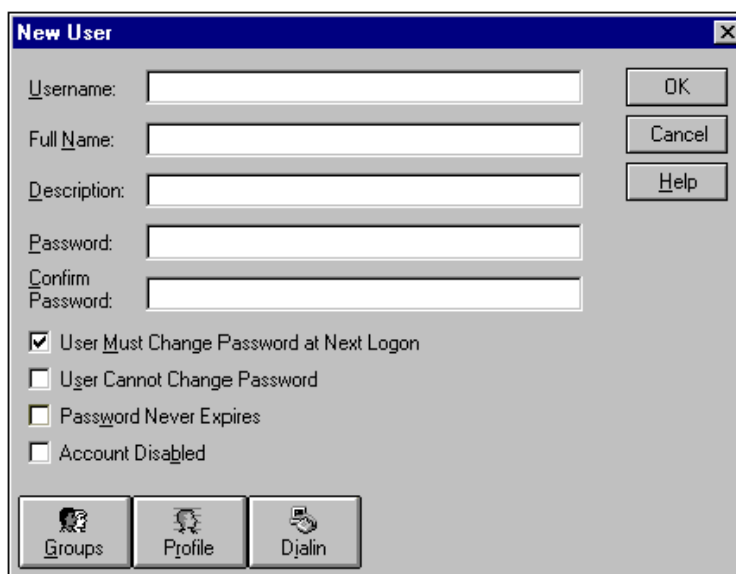
All electronic records generated by RESULT can be archived on a secure server such as a Windows system. The system owner or MIS/IT group must determine how the files will be archived and backed up and who has access to these records. It is also necessary to have a procedure to ensure that retrieval records can be read. Generally, this requires the system owner to convert records to a new format or to keep and maintain the tools for reading the records in their current format.

§11.10(d) *Limiting system access to authorized individuals.*

Using Windows secure logons is the preferred method for controlling access to the system. RESULT can be installed only on computers that have the Windows operating systems which ensure that you can control access to the system. The RESULT User's Guide provides details on computer requirements. A user profile is created with the User Manager in Windows, and each profile is associated with only one logon identification. Using the Windows User Manager, the RESULT software is installed only under user accounts that call for access to the system.

The logon feature of Windows allows system administrators to restrict system access to those who are authorized. To gain access to RESULT, users must log on to Windows and then re-enter their Windows passwords when launching RESULT. 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 manual or on-line help.)

The system administrator also can configure users' profiles to restrict their access to 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 configuration file of RESULT Operation can be accessed and changed only by those with RESULT administrator privileges, which are granted with the RESULT Operation User Manager.



*Example of New User dialog box in Windows User Manager
(Windows NT® example)*

§11.10(e) *Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.*

Every time an electronic record is created, modified, or deleted, information about that action is automatically logged to a database created by RESULT Operation. The entries into the database are date and time stamped and are assigned a unique identification number that represents the entry number in the database. (An operator name is also listed, along with a description of the action.) Older entries in the database cannot be overwritten, but the database is SQL compatible and can be queried using RESULT or other database applications such as MS Access. Because the audit trail is SQL compatible, it can be easily reviewed and copied by the FDA.

The audit log can also be used to detect backdating. When the log is sorted by key ID, the dates and times should be in chronological order. If they are not, it is a clear indication that backdating has occurred. (The system owner must establish a procedure for maintaining an audit trail log.)

The Windows event log, in addition to the audit log, can be used as an audit trail for monitoring operating system events such as file deletions and unauthorized log on attempts.

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

RESULT software has two distinct applications programs: RESULT Integration and RESULT Operation. A lab manager, or some other trained individual, uses RESULT Integration to create workflows.

A workflow is a series of tasks (such as collecting and archiving data) that an operator performs during sample analysis. In RESULT Integration, the workflow creator specifies the collection parameters, determines which electronic records will be archived, sets the location where archived records are stored, and decides if and when digital signatures will be used. (The option to use digital signatures is included to help ensure the integrity of the steps and events in workflows.)

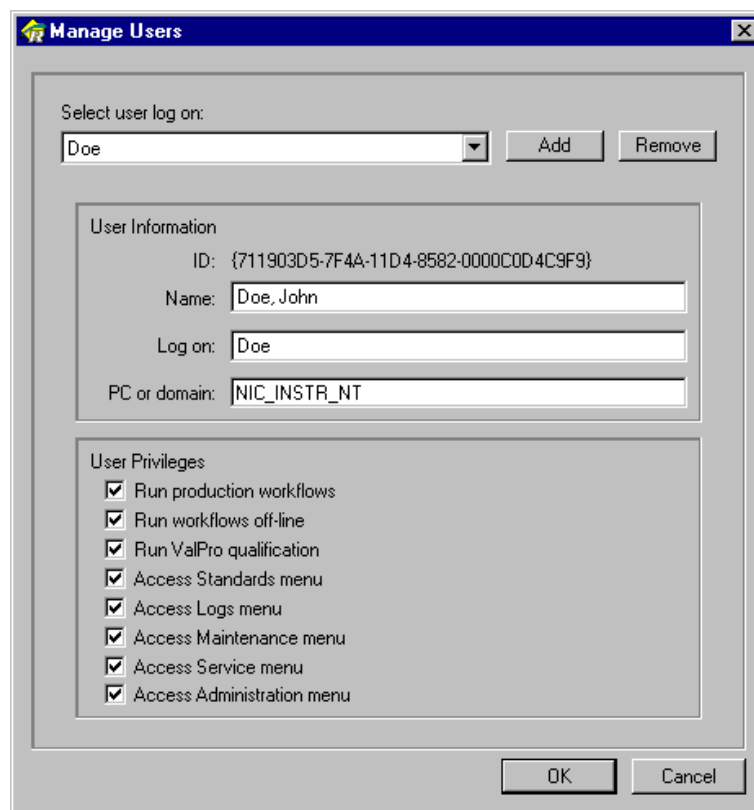
Once the workflow meets the requirements of the system owner, it is implemented in RESULT Operation, which is the application used by operators to run routine samples in a production environment. The RESULT Operation interface is easy to use. It provides operators with only the functions they need and can be configured to grant each user specific privileges. The operator is prompted step-by-step through an analysis based on the set of workflow tasks created in RESULT Integration. (A typical sequence for an analysis is to collect, measure, report, and then archive data.)

These features limited user access, controlled analysis events, and automatic data archiving reduce the potential for operator mistakes and help enforce the sequencing of events.

- §11.10(g) *Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.*

Because Windows security is embedded in the RESULT 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 system 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 RESULT Operation software. In addition, RESULT has a logon feature that can be used to control the functionality available to the operator. To use the logon feature, an administrator configures the Manage Users dialog box.



Manager Users dialog box in RESULT Operation

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

Spectrometer parameters are chosen from select lists during the creation of the workflow in RESULT Integration. In the workflow, the creator determines the collection parameters for each analysis. When the workflow is implemented in RESULT Operation, these same parameters are executed. The operator, who generally is not given access to RESULT Integration, cannot change the collection parameters, and the software and firmware restrict and check most of the spectrometer parameters.

- §11.10(i) *Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.*

Training classes on RESULT software and Thermo Electron's Antaris™ line of analyzers are available at Thermo Electron's development and manufacturing site in Madison, Wisconsin, Thermo Electron facilities throughout the world, and at your site. These courses are available to assist you in training those who maintain or use electronic record systems supplied by Thermo Electron.

To facilitate the training of your operators, RESULT Operation is able to incorporate electronic Standard Operating Procedures (SOPs) in the Adobe® Acrobat® format (pdf). These work instructions can be associated with functions in RESULT Operation, and the SOPs can be digitally signed using the features available in Adobe Acrobat version 4.0 or greater. (Refer to the Adobe Acrobat documentation for details on signing these files.)

Thermo Electron trains its developers and maintains training records according to internal quality procedures. A training matrix is maintained along with individual training records for each developer. Thermo Electron's Madison, Wisconsin site is ISO 9001:2000 certified and follows these guidelines when developing all products.

A training matrix is also maintained for Thermo Electron field service engineers, who are trained to maintain and service Thermo Electron Corporation products. These service engineers attend a comprehensive training course and must be re-certified on an annual basis.

§11.10(j) *The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.*

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

§11.10(k) *Use of appropriate controls over systems documentation including:*

§11.10(k1) *Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.*

The software includes manuals for operating and maintaining Thermo Electron analyzers and RESULT software, and the information in these manuals can be used to create SOPs.

Note It is the responsibility of the system owner to control the system documentation. ▲

§11.10(k2) *Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.*

Software and firmware, as well as on-line and printed documentation, contain version information that can be incorporated into the system owner's documentation control system. Information on the software and firmware version number can be obtained by running Instrument Status from the Maintenance menu in RESULT Operation. The system owner must implement a change control protocol for system documentation.

ValPro reports also contain version and signature information that can be incorporated into the system owner's documentation control system. (Information on the ValPro version number and signature information can be obtained by referring to the ValPro reports.)

§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.

Windows security is embedded as part of the RESULT software structure, and security is set up through the Windows security feature. The Windows logon and password, in conjunction with the password re-verification required when starting RESULT Operation, provide a way to control access to the RESULT software and an analyzer. Those responsible for maintaining system records must take adequate measures to ensure that RESULT complies in an open system. By following the guidelines in this document, RESULT will comply with the requirements for a closed system.

§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.*

(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).

Additional requirements for a handwritten or electronic signature are the printed name of signer, the date and time when signed, and the meaning of the signature (such as review or approval). The signature must be included as a part of any human readable form of an electronic record. All digital signatures produced by RESULT contain the information specified by the regulations, in addition to the signature. The signature is included as part of the human readable, 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 RESULT are directly linked to the electronic record. A check of an electronic record can verify if 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

Subpart C of 21 CFR 11 documents the regulations pertaining to the generation and use of electronic signatures.

§11.100 General requirements

This section of 21 CFR 11 details the general requirements for assigning and instituting electronic signatures.

§11.100(a) *Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*

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

§11.100(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.*

The system owner's policy for assigning Windows logons and passwords must comply with this requirement, which 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, then the digital

signature produced by RESULT will be unique. 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. (A procedure to ensure the requirements of §11.100 must be established by the organization or system owner.)

§11.200 Electronic signature components and controls.

This section of 21 CFR 11 details the components and controls required for using electronic signatures.

§11.200 (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.

Digital signatures used by RESULT are based on the user's logon and Windows password. The cryptographic service in Windows is used to generate the digital signature in RESULT, 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 Result software require entering a logon identification and a password.

- §11.200 (a) *Electronic signatures not based upon biometrics shall:*
- (2) *Be used only by their genuine owner.*
 - (3) *Be administered to ensure that attempted use of the electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.*

The system owner and administration must implement a protocol for using electronic signatures that ensures that requirements (2) and (3) are met.

- §11.200 (b) *Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.*

This requirement does not apply to RESULT because RESULT uses digital signatures based on the combination of a username and password, not on 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:*

- §11.300(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 ID code and password combinations are unique by issuing each user a unique logon identification.

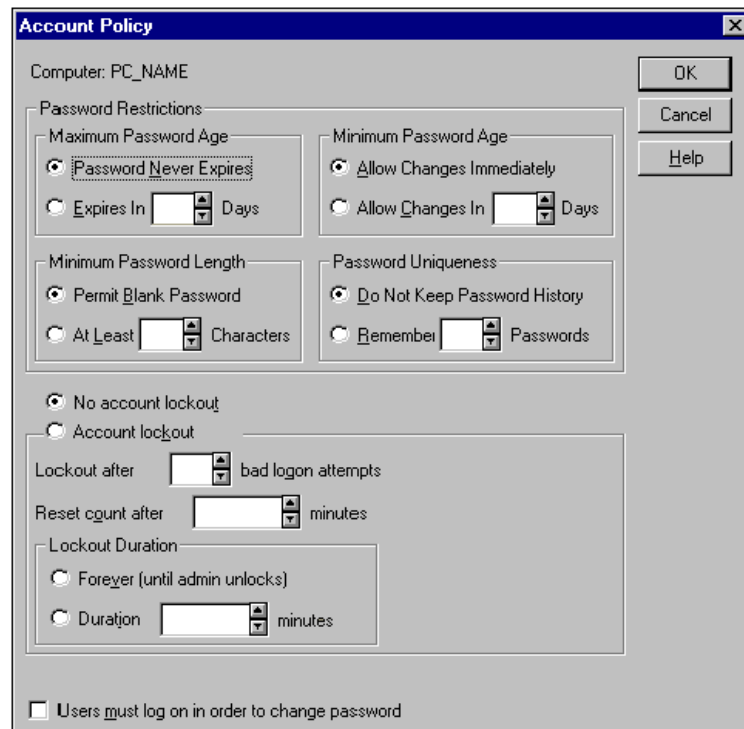
- §11.300(b) *Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).*

- §11.300(c) *Following loss management procedures to electronically de-authorize 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.*

- §11.300(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.*

The Windows security features simplify the process of periodically checking, recalling, and revising logons and passwords. (Transaction safeguards that prevent unauthorized access to the system are also available in Windows.) The event log can be configured to log attempts at unauthorized access, but the system administrator must establish procedures for loss management and checking ID codes and passwords.

A recommended method for preventing unauthorized use is to limit and log the number of failed logon attempts and to set up a password aging procedure that sets a limit on the length of time a password is valid.



*Example of Account Policy dialog box
(Windows NT version)*

§11.300(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.*

RESULT does not use cards or tokens to create identification codes, so this does not apply.

Summary

In summary, RESULT was designed and developed to comply with the requirements in the 21 CFR Part 11. Based upon Thermo Electron's interpretation of the regulations and on consultation with experts in the field, RESULT contains all the necessary tools required to assist you in complying with the regulations on electronic records and electronic signatures.



For More Information

For more information on the requirements of 21 CFR Part 11, go online to the FDA web site at www.fda.gov.

For more information on Thermo Electron Corporation products including RESULT software and the ValPro System Qualification package contact:

Thermo Electron Corporation
5225 Verona Road, Bldg. 5
Madison, WI 53711-4495

Telephone: 1-800-642-6538 (U.S.A.) or
+608-273-5015 (worldwide)
Fax: +608-273-5045 (worldwide)
E-mail: techsupport.analyze@thermo.com

You can also find information regarding Thermo Electron products by visiting the Thermo Electron web site at: www.thermo.com.

For the telephone and fax numbers of Thermo Electron subsidiaries and representatives, please refer to the Thermo Electron web site listed above.



RESULT Software 21 CFR Part 11 Compliance Document Disclaimer

We are providing this information to help you understand and address the 21 CFR Part 11 regulations and to explain how RESULT software meets these regulations. By providing this document, we are not recommending how to implement the regulations. Our customers are solely responsible for reading, understanding, interpreting, and implementing the regulations in the 21 CFR Part 11 with Thermo Electron products.

In providing you with the 21 CFR Part 11 Compliance statement contained in this document, Thermo Electron has taken reasonable measure to provide accurate information regarding the 21 CFR Part 11 compliance of our products. However, it must be understood that regulations and the enforcement of those regulations are continually changing, and we cannot guarantee that the information contained in this document is complete and current or that it applies to every situation.

For non-Thermo Electron products, whether obtained from us or our authorized distributors, please consult directly with the third-party product developer for the 21 CFR Part 11 compliance status of those products. In some cases we may pass along information that third parties have provided regarding the 21 CFR Part 11 compliance status of their products. We have not verified, will not verify, and will not accept any responsibility for the accuracy or completeness of such information.

The information in this document could contain technical inaccuracies or typographical errors and is subject to change without notice.

Thermo Electron Corporation, its employees, or its agents or representatives in connection with the information in this documents in no event shall be liable for indirect, special, consequential or incidental damages, including but not limited to loss of revenue, loss of profits, or loss of good will, regardless of whether we (a) have been informed of the possibility of such damages, or (b) are negligent.

Thermo Electron's obligations and responsibilities regarding our products are governed solely by the agreements under which they are sold or licensed. Nothing in this statement is intended to modify rights or obligations under any agreements or to create any new rights or obligations between us and our customers.

