# PTC's Windchill® PLM Software Facilitates Compliance with 21 CFR Part 11

## Proven Solution Enables the World's Most Demanding Medical Device Manufacturers to Comply with FDA Regulations

Windchill, PTC's Product Lifecycle Management (PLM) solution, provides comprehensive software capabilities that Medical Device manufacturers need to comply with 21 CFR Part 11. By implementing Windchill's appropriate procedural controls and business process, you have the right architecture to support complete and highly configurable solutions that ensure compliance with all applicable aspects of the Part 11 regulation.

The following matrix maps each requirement in Part 11 to Windchill's capabilities that support compliance. Below the matrix is an appendix that further explains Windchill's capabilities regarding specific areas of the regulation.

| Subpart B–Electronic Records | Windchill | Additional Remarks | References |
|---|---|---|---|
| **Sec.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: | √ | | |
| (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | √ | Windchill development follows a CMMI L2 process and has been validated many times by leading medical device companies. | See Appendix Section 11.10 Control for Closed Systems–Validation |
| (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. | √ | | See Appendix Section 11.10 Control for Closed Systems–Complete Copies |
| (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | √ | | |
| (d) Limiting system access to authorized individuals. | √ | Medical Product organizations must define SOPs and practices that address this requirement. | See Appendix Section 11.10 Control for Closed Systems–System Access |
| (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. | √ | Medical Product organizations must define SOPs and practices that address this requirement. | See Appendix Section 11.10 Control for Closed Systems–Audit Trails |
| (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | √ | | |
| (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. | √ | | |

| | Windchill | Additional Remarks | References |
|---|---|---|---|
| (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | √ | Data inputs are verified by Windchill. | |
| (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. | NA | Medical Product organizations must define SOPs and practices that address this requirement. | |
| (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. | NA | Medical Product organizations must define SOPs and practices that address this requirement. | |
| (k) Use of appropriate controls over systems documentation including: | NA | | |
| (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. | NA | Medical Product organizations must define SOPs and practices that address this requirement. | |
| (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | √ | Windchill creates an audit trail. Medical Product organizations must define procedures that address this requirement. | |
| **Sec.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. | √ | Windchill supports encryption and authentication with the use of Hypertext Transfer Protocol Secure (HTTPS) and Secure Sockets Layer (SSL) connections. | See Appendix Section 11.30 Control for Open Systems–Open System |
| **Sec.11.50 Signature Manifestations** | | | |
| (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: | √ | | See Appendix Section 11.50 Signatures Manifestations–Manifestations |
| (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. | √ | Configured based on intended use. | |
| (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). | √ | All transactions in Windchill are audit trailed. | |
| **Sec.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. | √ | | See Appendix Section 11.70 Signature/Record Linking–Linking |

| Subpart C – Electronic Signatures | Windchill | Additional Remarks | References |
|---|---|---|---|
| **Sec.11.100 General Requirements** | | | |
| (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. | √ | | See Appendix Section 11.100 Electronic Signatures – Unique Signature |
| (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. | **NA** | Medical Product organizations must define SOPs and practices that address this requirement. | |
| (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. | **NA** | Medical Product organizations must define SOPs and practices that address this requirement. | |
| (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. | **NA** | Medical Product organizations must define SOPs and practices that address this requirement. | |
| (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. | **NA** | Medical Product organizations must define SOPs and practices that address this requirement. | |
| **Sec.11.200 Electronic Signature Components and Controls** | | | |
| (a) Electronic signatures that are not based upon biometrics shall: | √ | | See Appendix Section 11.200 Electronic Signature Components and Controls – Biometrics |
| (1) Employ at least two distinct identification components such as an identification code and password. | √ | | See Appendix Section 11.200 Electronic Signature Components and Controls – Two Identifications |
| (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. | √ | | See Appendix Section 11.200 Electronic Signature Components and Controls – Series Signatures |
| (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. | √ | | |
| (2) Be used only by their genuine owners; and | √ | Medical Product organizations must define SOPs and practices to manage passwords. | |

| | Windchill | Additional Remarks | References |
|---|---|---|---|
| (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. | √ | Medical Product organizations must define SOPs and practices to manage passwords.<br>Windchill provides audit trail of all actions, including administrator actions. | |
| (b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. | √ | Windchill uses its authentication mechanism to be compatible with third-party biometric devices and applications. | |
| **Sec. 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. | √ | | See Appendix Section 11.300 Controls for Identification Codes/Passwords – Unique Identification |
| (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | √ | Operating software and third-party solutions.<br>Company-defined SOP and practices.<br>Windchill uses its authentication mechanism to be compatible with third-party biometric devices and applications. | See Appendix Section 11.300 Controls for Identification Codes/Passwords – System Safeguards |
| (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. | **NA** | Medical Product organizations must define SOPs and practices that address this requirement. | |
| (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. | √ | Operating software and third-party solutions. | |
| (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. | **NA** | Medical Product organizations must define SOPs and practices that address this requirement. | |

# Appendix

## Sec.11.10 Controls for Closed Systems:

### Validation

PTC follows the CMMI Level II process in developing and testing our software, with each component having been extensively tested. Windchill has passed customers' numerous audits, with Windchill having been successfully installed and validated by many leading medical device manufacturers to meet their unique needs, configurations and intended use. Windchill implementations have undergone multiple FDA audits in support of the Manufacturer's Quality System Regulations.

### Complete Copies

All records and logs produced by Windchill can be rendered in human and electronic forms that are suitable for inspection, review or copying.

### System Access

System access is strictly controlled through the use of unique identification and passwords. In addition, system access is further controlled by a permissions hierarchy that limits access to each system function based on role or job classification as defined by the customer's business needs.

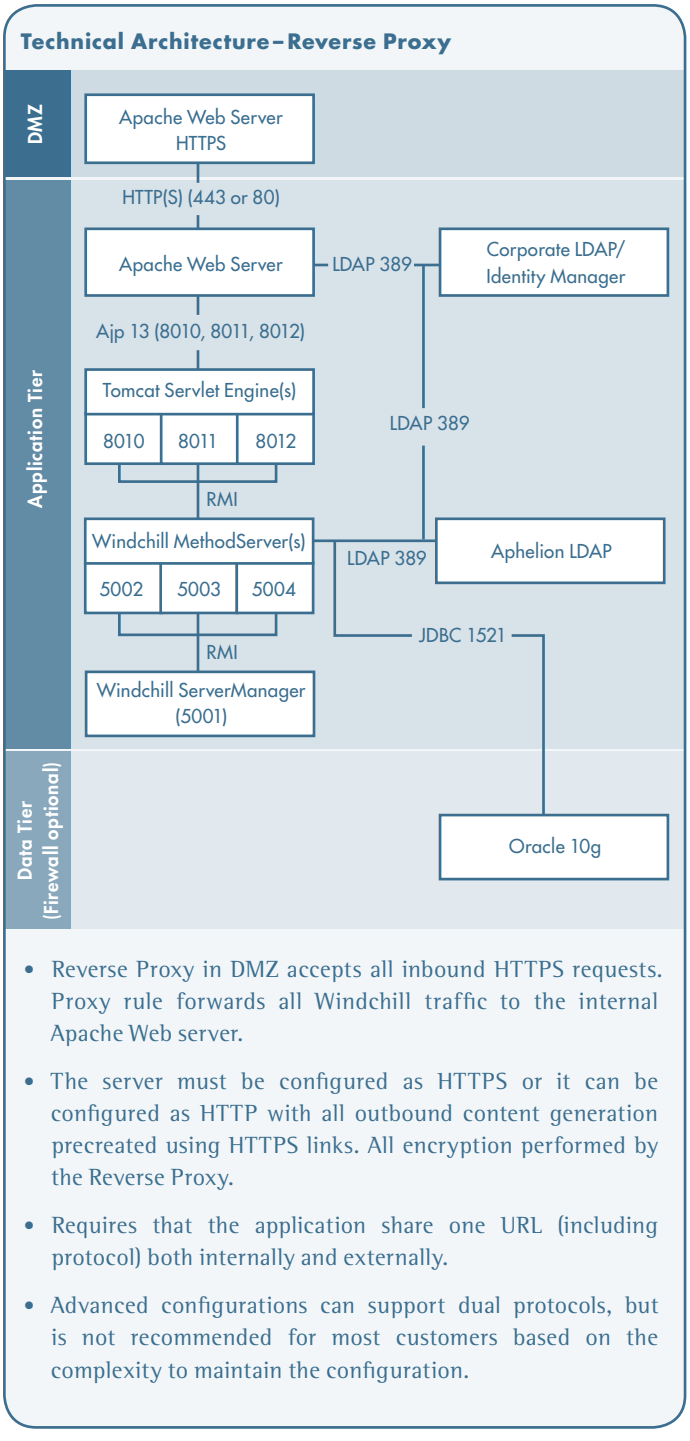
### Audit Trails

Windchill maintains a complete time-stamped and computer-generated audit trail of all system transactions, including those performed by the system administrator. This capability includes secure, computer-generated time stamps of user entries and modifications. In addition, the system uses version control and checkout/checkin locks to ensure control over documents.

## Sec.11.30 Controls for Open Systems:

### Open System

Windchill supports encryption and authentication with the use of Hypertext Transfer Protocol Secure (HTTPS) and Secure Sockets Layer (SSL) connections. This solution supports the requirements of Part 11 by ensuring the integrity and confidentially of records. HTTPS access to Windchill from outside the secure network is typically enforced by Port Forwarding or more complex techniques like Reverse Proxy. In this case, the only port enabled for forwarding from the firewall/router is a secure HTTPS port. You can now access Windchill only through an encrypted connection from the public Internet by using the IP address of the router.




- Reverse Proxy in DMZ accepts all inbound HTTPS requests. Proxy rule forwards all Windchill traffic to the internal Apache Web server.
- The server must be configured as HTTPS or it can be configured as HTTP with all outbound content generation precreated using HTTPS links. All encryption performed by the Reverse Proxy.
- Requires that the application share one URL (including protocol) both internally and externally.
- Advanced configurations can support dual protocols, but is not recommended for most customers based on the complexity to maintain the configuration.

**Figure 1**: Sample Windchill configuration to meet Open System requirements

### Sec.11.50 Signature Manifestations:

#### Manifestations

When approving a document electronically, Windchill users provide their printed name, date and time when approved, and the approver's role. The meaning of the signature can be defined by system roles and further supplemented by the use of comments based on system configuration.

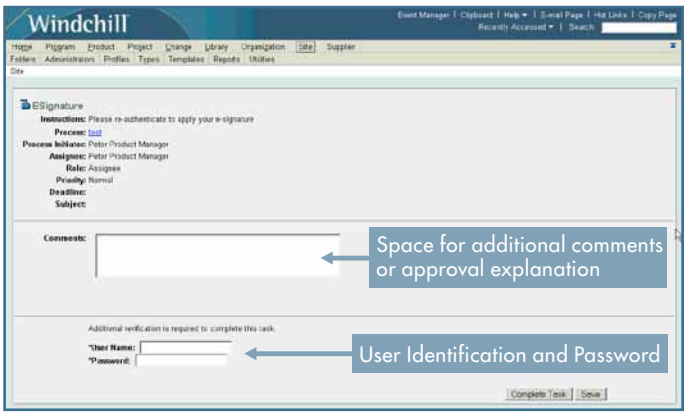



**Figure 2**: Windchill screenshot showing signature manifestation

### Sec.11.70 Signature/Record Linking:

#### Linking

Electronic signatures are secured and linked with file-name linking – available as a readable document, to ensure compliance. Each file has a unique identifier, and a complete approval history can be produced.

### Sec.11.100 General Requirements:

#### Unique Signature

Windchill does not allow duplicate user identifications and ID/password combinations for system access or document approval. This capability should be supplemented with customer-defined policies and practices that do not permit an identification to be reused.

### Sec.11.200 Electronic Signature Components and Controls:

#### Biometrics

Windchill supports biometric document approval through third-party solutions.

#### Two Identifications

Two distinct and unique forms of identification (user name and password) are required both for (a) system access and (b) to submit an electronic signature.

#### Series Signatures

To further strengthen Part 11 compliance, Windchill requires both user identification and password to be executed for each approval.

### Sec.11.300 Controls for Identification Codes/Passwords:

#### Unique Identification

The system will not allow two individuals to have the same identification and password.

#### System Safeguards

Windchill functionality supports operating-platform safeguards and security, in addition to operating with third-party solutions like Site Minder. This approach ensures system integrity while enhancing the user experience through single sign-on practices, which facilitate long-term, comprehensive system security and compliance.

## For More Information

Learn more about Windchill and PTC's support for 21 CFR Part 11 at ptc.com/windchill.

© 2010, Parametric Technology Corporation (PTC). All rights reserved. Information described herein is furnished for informational use only, is subject to change without notice, and should not be construed as a guarantee, commitment, condition, or offer by PTC. PTC, the PTC logotype, Windchill and all PTC product names and logos are trademarks or registered trademarks of PTC and/or its subsidiaries in the United States and in other countries. All other product or company names are property of their respective owners.

5590-Windchill-21-CFR-Part-11-TS-EN-0710