

White Paper:

21 CFR Part 11:
MasterControl Product Positioning

Video: Creating a Paperless Process



View Customer Video Now
Click here to launch



If you like our white papers, you'll love our products.
See what our customers say about MasterControl products.

**SUBPART B
ELECTRONIC RECORDS**

21 CFR Part 11 Section	Regulation Summary	MasterControl Feature
11.10	Ensure authenticity, integrity, and when appropriate, confidentiality of electronic records	<p>MasterControl provides a system administration feature that defines permissions for each user and for electronic records in the system. There are more than 100 permissions available in MasterControl and are assigned at the administrator level.</p> <p>System administrators have all permissions and are able to restrict user access to records as is necessary and appropriate. Actions taken against any record in the MasterControl system are captured in the MasterControl audit trail.</p>
11.10	Minimize possibility of repudiation by signer	MasterControl has numerous levels of security to ensure the authenticity of each user in the system. Each user has a unique user ID and login password that the user uses to gain access to the system. Additionally, in order to sign off on any record, they must use a different “approval” password unique to this individual user. All user IDs and passwords are encrypted for security.
11.10 (a)	Validate the system and ensure ability to detect invalid or altered records	<p>MasterControl offers an exhaustive set of IQ, OQ, and PQ test protocols to assist customers with software validation. Updated protocols are provided with each and every system build and revision.</p> <p>Changes that are made to a record or record metadata are captured in the audit trail with a field provided for “reason for change.”</p>

11.10 (b)	Provide ability to generate accurate and complete records in both human readable and electronic form	Records along with associated metadata can be copied electronically, viewed electronically or printed to paper. Reports can also be printed from the system or exported to other tools such as spreadsheets.
21 CFR Part 11 Section	Regulation Summary	MasterControl Feature
11.10 (c)	Protect records to enable accurate and ready retrieval	MasterControl protects all electronic records through its comprehensive permission system and unique storage technology. Based on privilege, users can utilize MasterControl search tools to retrieve records that have been identified as permissible.
11.10 (d)	Limits system access to authorized individuals	MasterControl limits login access, and record access through its permission system. The administrator at the system level assigns permissions.
11.10 (e)	Creates secure, computer-generated, time-stamped audit trails	MasterControl audits events associated with a record. These auditable events are time- and date-stamped and cannot be altered by anyone including the system administrator.
11.10 (f)	Use of operational system checks-- as appropriate--to enforce permitted sequencing of steps and events	MasterControl is an event driven system. Routing of records can be enforced ensuring proper sequencing of steps and events.
11.10 (g)	Perform authority checks of users Check use of the system, signing of records or altering of a record	MasterControl checks user ID and password at login and each record is protected based on rights. Signature is performed using a unique ID and password. Any changes made to a record are time- and date-stamped in the audit trail and access is based on a unique ID and password.
11.10 (h)	Use of device checks to determine validity of the source of data input	The ability to input data into MasterControl is a “rights-based” privilege. Any time a record is created, the user ID and information are captured in the audit trail.

11.10 (i)	Determination that persons using the electronic system have been properly trained to perform their assigned tasks	MasterControl has classroom, online training and training materials available for users from system administrators to general users. System administrator training is conducted at MasterControl's corporate site training center and/or on-site at a user's location. After administrator training, user training takes place at the client site. Training courses are given for each level of user to ensure that each and every user can perform their assigned tasks inside the MasterControl system.
11.10 (j)	Establish and follow written policies against falsification of records under their electronic signature	Organizations should develop internal policies in regard to user ID and password confidentiality. MasterControl does not allow the system administrator or any single user to change signature credentials alone, thus eliminating the ability of anyone to falsify an electronic signature.
11.10 (k)	Appropriate controls over system documentation	Organizations should develop internal policies in regard to controls over system documentation. MasterControl maintains revision and change control over system documentation that is made available to the customer. Customers can use their own MasterControl application to control and maintain access to these and other system documents that may be created.
21 CFR Part 11 Section	Regulation Summary	MasterControl Feature
11.30	Implement document encryption for record confidentiality	All controlled documents added to MasterControl are encrypted using industry standard cryptography to prevent tampering with the files on the file system outside of MasterControl. All passwords and electronic signatures are encrypted using industry-standard encryption.

11.30	Use digital signatures for a record authenticity and integrity	MasterControl provides electronic signature information based on the user's unique id and password for electronic signature authenticity and integrity.
Section 11.50 Signature Manifestations.		
11.50 (a)	Signed electronic records must contain a name as well as the date, time and meaning of a signature	Records in MasterControl that are signed electronically capture the user name, time/date and meaning of signature.
11.50 (b)	Items in 11.50 (a) must appear on every human readable form of the electronic record	Master Control displays user name, time/date and meaning of signature on the readable form of the record. This signature information is displayed on the record whether viewed electronically or when printed from the system by a user.
Section 11.70 Signature/record linking.		
11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records	In MasterControl every signature is directly linked to that specific record only. This signature information cannot be tampered with after approval. Whether viewing on screen or via printed copy there is a link between the specific document and its corresponding electronic signature.

SUBPART C

ELECTRONIC SIGNATURES 11.100

21 CFR Part 11 Section	Regulation Summary	MasterControl Feature
11.100 (a)	Electronic signatures shall be unique and shall not be re-used or re-assigned	MasterControl tracks each and every signature combination and does not allow duplication or reassignment of the user ID and signature combination.
11.100 (b)	Organizations must verify identity of individuals receiving electronic signatures	Organizations should develop internal policies to verify the identity of the individual before providing access.

11.100 (c)	Organizations must certify to the FDA their intent to use electronic signatures	The standard MasterControl package notifies customers of this requirement and provides an implementation note, which provides a draft script for FDA notification.
21 CFR Part 11 Section	Regulation Summary	MasterControl Feature
11.200 (a) (1)	Non-biometric e-signatures must have at least two components	MasterControl requires a non-biometric signature to have a user ID and password to log onto the system as well as a separate password for signature. The client has the option of configuring the length of this password, alphanumeric combination or whatever they see fit to maintain the highest levels of security for their system.
11.200 (a) (1) (i)	Continuous session: first signing must use all components; subsequent signings can use one component	MasterControl again requires the use of a user ID and password upon entering the system and a private password component for every subsequent signing.
11.200 (a) (2)	Non-biometric electronic signatures must be used only by the genuine owner	User ID and password combination are unique to one user only. However the organization should have policies in place to eliminate the risk of password sharing and or password protection.
11.200 (a) (3)	Attempted use of non-biometric e-signatures requires collaboration of two or more people	MasterControl encrypts passwords so only the user will know his or her password. For a password to be changed in the system by an administrator there must be two signatures. Only users with the 'certify password' right in the system will be able to approve password changes.
11.200 (b)	Biometric e-signatures must be usable only by the genuine owner	Biometric signatures can be used in MasterControl based on a client's needs, but may require customized integration, depending on the specific biometric application.

21 CFR Part 11 Section	Regulation Summary	MasterControl Feature
11.300 (a)	Maintain uniqueness of “ID code & password” combination	<p>MasterControl has specific rules built into its security as follows:</p> <p>No user in the system can have the exact same combination of ID and signature. The system tracks this and simply will not let it happen.</p> <p>The ID and secondary password are case sensitive and their length can also be specified by the user. Alpha and numeric character requirements as well as the number of days until expiration can also be specified by the user.</p>
11.300 (b)	Periodically check ID code and password. Password aging	MasterControl is configurable and the system administrator is able to determine password and electronic signature expiration periods.
11.300 (c)	Manage lost or stolen tokens, cards or other devices and manage replacement issues	Users who have certified password rights must change lost or stolen passwords. The time and date is logged when a password has been changed.
11.300 (d)	Prevent unauthorized use of passwords and the codes; detect and immediately report any such attempts	MasterControl notifies the administrator when an incorrect password has been tried. The system is configurable in regard to number of times an account can have an incorrect password before the account is completely locked out, and what actions are taken.
11.300 (e)	Test devices tokens, cards initially and periodically for proper function	If a client goes to a biometric form of signature the system would have the same security in place that is again configurable by the organization using MasterControl. Testing would be the responsibility of the customer.

About MasterControl Inc.

MasterControl Inc. produces software solutions that enable regulated companies to get their products to market faster, while reducing overall costs and increasing internal efficiency. MasterControl securely manages a company's critical information throughout the entire product lifecycle. Our software is known for being easy to implement, easy to validate and easy to use. MasterControl solutions include quality management, document management/document control, product lifecycle management, audit management, training management, bill of materials, supplier management, submissions management, and more. Supported by a comprehensive array of services based on industry best practices, MasterControl provides our customers with a complete information management solution across the entire enterprise. For more information about MasterControl, visit www.mastercontrol.com, or call: 800-825-9117 (U.S.); +44 1256 325 949 (Europe); or 03-6801-6147 (Japan).

Related Videos



[FDA Compliance](#)



[Improving Quality](#)



MasterControl Inc.

Corporate Headquarters:

MasterControl Inc.

6322 S. 3000 E. Ste. 110

Salt Lake City, UT 84121

United States

Phone: 800.825.9117

Fax: 801.942.7088

www.mastercontrol.com

Asian Headquarters:

MasterControl KK

Aios Akihabara 702

3-2-2 Ueno Taito-ku

Tokyo 110-0005

Japan

Phone: +81 (0) 3 6801 6147

Fax: +81 (0) 3 6801 6148

www.mastercontrol.com

European Headquarters:

MasterControl Global Limited

First Floor North Wing

Matrix House

Basing View

Basingstoke

RG21 4FF

United Kingdom

Phone: +44 (0) 1256 325 949

Fax: +44 (0) 1256 325 289

www.mastercontrolglobal.co.uk

Germany Office

Mendelstrasse 11

48149 Muenster

Germany

Phone: +49 (0) 251 980 2140

Fax: +49 (0) 251 980 2149

www.mastercontrolglobal.de

Email: info@mastercontrol.com