# 21CFR Requirement Checklist

FTTA 21CFR Data Loggers are available in either standalone USB or WiFi formats. Please find below 21CFR compatibility checklists for both options.

✓ = Fully Compliant ⓘ = Compliant with user control via SOPs (Standard Operating Procedures)

## WiFi 21CFR Cloud *(see page 11 for Standalone 21CFR USB)*

### Sec. 11.10 Controls for Closed Systems

| 21CFR Part 11 requirement | Does the FTTA 21CFR Cloud meet this requirement? | Comments |
|---|---|---|
| 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.<br><br>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 FTTA 21CFR Cloud provides both Device and System Audit trails detailing user activities. |
| 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. 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. | ✓ | The FTTA 21CFR Cloud can be used to generate complete copies of all records in both human readable and electronic form - which can be used for inspection, review and copying by the agency. |
| c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | ✓ | The FTTA 21CFR Cloud records are stored in a Database with controlled access, which are readily and securely retrievable using the FTTA web user interface. Data is read-only and cannot be accessed in any other way. Each action to delete, print, export or add comments to data, is further controlled by the entry of an Approver's credentials. The Approver must have sufficient privileges to perform the selected action. |
| d) Limiting system access to authorized individuals. | ✓ | Access to the FTTA 21CFR Cloud is under user email and password control. Administrators grant access to chosen users only, and assign usage privileges to each. Assignable privileges include, the ability to view, print and export data. Key actions are further controlled by the entry of an Approver's credentials. The Approver must have sufficient privileges to perform the selected action. |
| 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. | ✓ | FTTA 21CFR Cloud generates a System Audit trail, detailing all user activities.<br><br>For more information on what is included in audit trail, please see table 1.<br><br>Data cannot be overwritten or altered however, data and the System Audit can be deleted by an Administrator. All delete actions are recorded in the System Audit. |

| 21CFR Part 11 requirement | Does the FTTA 21CFR Cloud meet this requirement? | Comments |
|---|---|---|
| f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | ✓ | The FTTA 21CFR Cloud is designed to ensure that the user is limited to performing one function at a time, and in the correct order. |
| 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. | ✓ | Yes - please see Sec. 11.10 d). |
| h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | N/A | Not applicable to FTTA 21CFR Cloud. |
| 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. | ✓ ! | This is the user's responsibility. The WiFi-21CFR device is supplied with a Quick Start Guide and online Help resources, and a thorough help file is included within the software. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| k) Use of appropriate controls over systems documentation including: | | |
| 1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. | ✓ ! | This is the user's responsibility. The WiFi-21CFR device is supplied with a Quick Start Guide, and a thorough help file is included within the software. |
| 2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | ✓ ! | The FTTA 21CFR Cloud provides both Device and System Audit trails to record system changes and actions carried out. In-house procedures are the user's responsibility.<br>Users need to have their own Standard Operating Procedure. |

## Sec. 11.50 Signature Manifestations

| 21CFR Part 11 requirement | Does the FTTA 21CFR Cloud meet this requirement? | Comments |
|---|---|---|
| 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; | ✓ | Yes - please see Sec. 11.10 e). |
| 2) The date and time when the signature was executed; and | ✓ | Yes - please see Sec. 11.10 e). |
| 3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. | ✓ | Yes - please see Sec. 11.10 e). |

| | | |
|---|---|---|
| b) The items identified in paragraphs a1), a2), and a3) 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). | ✓ | Yes - please see Sec. 11.10 e). |

## Sec. 11.70 Signature/Record Linking

| 21CFR Part 11 requirement | Does the FTTA 21CFR Cloud meet this requirement? | Comments |
|---|---|---|
| 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. | ✓ | Yes - please see Sec. 11.10 e). |

## Subpart C - Electronic Signatures
## Sec. 11.100 General Requirements

| 21CFR Part 11 requirement | Does the FTTA 21CFR Cloud meet this requirement? | Comments |
|---|---|---|
| a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. | ✓ | FTTA 21CFR Cloud users create their own password for their account. Each Sign-In Email address must be unique. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |

## Sec. 11.200 Electronic Signature Components and Controls

| 21CFR Part 11 requirement | Does the FTTA 21CFR Cloud meet this requirement? | Comments |
|---|---|---|
| a) Electronic signatures that are not based upon biometrics shall: | | |
| 1) Employ at least two distinct identification components such as an identification code and password. | ✓ | The FTTA 21CFR Cloud uses Email and Password at Sign-In and Email and Password of an Approver, at the time key actions are being performed. |
| 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. | ✓ | On the FTTA 21CFR Cloud, each and every key action requires entry of both Email address and Password as the Approval signature. |
| 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. | ✓ | On the FTTA 21CFR Cloud, each and every key action requires entry of both Email address and Password as the Approval signature. |
| 2) Be used only by their genuine owners; and | ✓ | Please see Sec. 11.100 a). |
| 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. | ✓ | Please see Sec. 11.100 a).<br>Attempts made to Approve an action, by a user without a sufficiently high user privilege level, will be recorded in the System Audit. |
| b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. | N/A | |

## Sec. 11.300 Controls for Identification Codes/Passwords

| 21CFR Part 11 requirement | Does the FTTA 21CFR Cloud meet this requirement? | Comments |
|---|---|---|
| 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. | ✓ | Please see Sec. 11.100 a). |
| b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | ✓ | An Administrator can change any user's registered Email address or password at any time. They can immediately deny system access to a user by permanently deleting the user and or temporarily change their password. |

| | | |
|---|---|---|
| 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. |  | Users can be deleted or their privileges changed by an Administrator. In the event that a user forgets their password, a reset link can be sent to the user's registered email address. It is the user's responsibility to make sure this is covered in their Standard Operating Procedure. |
| 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. |  | Attempts made to Approve an action, by a user without a sufficiently high user privilege level, will be recorded in the System Audit. |
| 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. |  | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |

## System Audit

All System Audit entries are Date/Time and contain the Full Name and Email address of the Signed-In User and the user giving Approval. The Approver must have the required privilege level to complete the operation.

If the user attempts to complete an action requiring Approval but has an insufficient privilege level, the attempted action is recorded in the System Audit.

| Action | System Audit Entry | Approval Required | User Privilege Required |
|---|---|---|---|
| Devices : | | | |
| Archive/Clear/Delete a device | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>List of Archived/Cleared/Deleted Devices - Names and MAC addresses |  | Administrator |
| Change Device Settings | None | | Manage Devices |
| View Data : | | | |
| Other Sessions : | | | |
| Export Device Audit | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Device Name and MAC<br>Document ID |  | Print & Export Device Data |
| Graph : | | | |
| Export | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Start & End Time/Date of data<br>Document ID |  | Print & Export Device Data |
| Print | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Start & End Time/Date of data<br>Document ID |  | Print & Export Device Data |

| Action | System Audit Entry | Approval Required | User Privilege Required |
|---|---|---|---|
| Data : | | | |
| Add a Comment | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Time/Date of data value<br>Data Value(s)<br>Comment | ✓ | Administrator |
| Export | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Start & End Time/Date of data<br>Document ID | ✓ | Print & Export Device Data |
| Event Logs : | | | |
| Clear Log | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>List of Devices - Names and MAC | ✓ | Administrator |
| Export | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Start & End Time/Date of Log<br>List of Devices - Names and MAC<br>Document ID | ✓ | Administrator |
| Send This Log | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Start & End Time/Date of Log<br>List of Devices - Names and MAC<br>Recipient : Email Address<br>Document ID | ✓ | Administrator |
| Reset Alarm | None | | Manage Devices |
| New Device added (New Devices) | None | | Manage Devices |
| Administration : | | | |
| Users : | | | |
| Create New User (pending user email address verification) | None | | Administrator (implied) |
| Edit User : Full Name | None | | Administrator (implied) |
| Edit User : Email Address | None | | Administrator (implied) |
| Edit User : Password | None | | Administrator (implied) |
| Edit User : User Privileges | None | | Administrator (implied) |
| Delete User | None | | Administrator (implied) |
| Locations : | | | |
| Create New Location | None | | Administrator (implied) |
| Edit Location | None | | Administrator (implied) |

| Action | System Audit Entry | Approval Required | User Privilege Required |
|---|---|---|---|
| Delete Location | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Name of Location(s) affected.<br>List of Archived/Cleared/Deleted Devices - Names and MAC addresses | ✓ | Administrator (implied) |
| Archive Location | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Name of Location(s) affected.<br>List of Archived/Cleared/Deleted Devices - Names and MAC addresses | ✓ | Administrator (implied) |
| Change Users belonging to a Location | None | | Administrator (implied) |
| System Audit : | | | |
| Delete part or all of the System Audit | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Amount of System Audit retained | ✓ | Administrator (implied) |
| Export System Audit | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Audit period or Start & End Time/ Date<br>File Format<br>Time Zone<br>Document ID | ✓ | Administrator (implied) |
| Settings : | | | |
| Change Auto Sign-Out time | Time/Date stamp<br>Approvers Full Name & Email<br>Signed-In user's Full Name & Email<br>Old and New Auto Sign-Out time | ✓ | Administrator (implied) |
| User Sign In | None | | None |
| User Sign Out | None | | None |
| Account : | | | |
| Account Details : | | | |
| Account Name | None | | Acct Administrator (implied) |
| Company Name | None | | Acct Administrator (implied) |
| Address | None | | Acct Administrator (implied) |
| Town/City | None | | Acct Administrator (implied) |
| State/County | None | | Acct Administrator (implied) |
| Zip/Postcode | None | | Acct Administrator (implied) |
| Country | None | | Acct Administrator (implied) |
| Time Zone | None | | Acct Administrator (implied) |
| Automatically adjust daylight saving time | None | | Acct Administrator (implied) |
| Billing Details | | | |
| Name | None | | Acct Administrator (implied) |
| Address | None | | Acct Administrator (implied) |

| Action | System Audit Entry | Approval Required | User Privilege Required |
|---|---|---|---|
| Town/City | None | | Acct Administrator (implied) |
| State/County | None | | Acct Administrator (implied) |
| Zip/Postcode | None | | Acct Administrator (implied) |
| Country | None | | Acct Administrator (implied) |
| Account type changed (Up/Downgrade) | None | | Acct Administrator (implied) |
| My Settings : | | | |
| Change Date format | None | | None |
| Change Time format | None | | None |
| Change Password | None | | None |
| Change Email Address | None | | None |
| Reduce the number of emails I get | None | | None |
| Insufficient Privilege | | | |
| Approval Failed: Any Action requiring Approval | Time/Date stamp<br>Full Name & Email entered<br>Signed-In user's Full Name & Email<br>Attempted Action | ✓ | Administrator |

## Example System Audit

**Document ID: 2-89B4EB Approved by: Tim Liversage (tim.liversage@winstanleyhc.com) 14/04/2016 11:52:27 ((GMT) Dublin, Edinburgh, Lisbon, London)**

# SYSTEM AUDIT

**Exported on 14/12/2015 10:19 (UTC-03:00 Greenland) by David Browlands (david.browlands@winstanleyhc.com)**
**Document ID : 2-89B4EB**
**Approved by Tim Liversage (tim.liversage@winstanleyhc.com)**

**Times shown are referenced to Time Zone: (GMT) Dublin, Edinburgh, Lisbon, London**

| | | | | |
|---|---|---|---|---|
| Audit Period | 12/12/2015 00:00 | to | 13/12/2015 00:00 | |
| Account | Winstanley Health Foods (21CFR PROFESSIONAL Tier 2) | | | |

| | | | |
|---|---|---|---|
| Date/Time | 13/12/2015 23:13 | Clear Device Data | |
| Signed-In User | Tim Liversage (tim.liversage@winstanleyhc.com) | Approved by | Tim Liversage (tim.liversage@winstanleyhc.com) |
| Comments | Device: Freezer 001/A (MAC 98:8B:AD:00:1D:74)<br>Device: Freezer 023/Sa (MAC 98:8B:AD:00:20:01) | | |
| Date/Time | 13/12/2015 22:22 | Export Device Audit | |
| Signed-In User | David Browlands (david.browlands@winstanleyhc.com) | Approved by | Tim Liversage (tim.liversage@winstanleyhc.com) |
| Comments | Device: Large Store (MAC 98:8B:AD:01:23:14)<br>Document ID : 3-54AAE1 | | |
| Date/Time | 13/12/2015 22:21 | Approval Failed | |
| Signed-In User | David Browlands (david.browlands@winstanleyhc.com) | Approved by | |
| Comments | Attempted Action: Export Device Audit by Paul Kenward (paul.kenward@larasian.co.uk) | | |
| Date/Time | 13/12/2015 22:21 | Print Graph | |
| Signed-In User | Edna Clouds (edna.clouds@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Freezer 001/A (MAC 98:8B:AD:00:1D:74)<br>Start: 11/12/2015 00:00 End: 12/12/2015 00:00<br>Document ID : 1-22CA40 | | |
| Date/Time | 13/12/2015 08:21 | Auto Sign-Out time changed | |
| Signed-In User | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Was: 10 minutes Is: 5 minutes | | |
| Date/Time | 13/12/2015 07:01 | Delete some or all of the System Audit | |
| Signed-In User | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Only System Audit entries from the last 7 days were retained. All other entries were deleted. | | |
| Date/Time | 13/12/2015 06:40 | Send Event Log | |
| Signed-In User | Anita House (anita.house@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Cold Store 4 (MAC 98:8B:AD:00:1D:33)<br>Device: Cold Store 2 (MAC 98:8B:AD:00:20:45)<br>Device: Cold Store 3 (MAC 98:8B:AD:00:33:56)<br>Device: Cold Store 1 (MAC 98:8B:AD:00:10:9A)<br>Log Start: 01/12/2015 00:00 Log End: 11/12/2015 00:00<br>Recipient: frank.sidebottom@bigfrankshealthfoods.com<br>Document ID : 0-996ef0 | | |
| Date/Time | 13/12/2015 06:32 | Export System Audit | |
| Signed-In User | Anita House (anita.house@winstanleyhc.com) | Approved by | Tim Liversage (tim.liversage@winstanleyhc.com) |
| Comments | Start: 01/12/2015 00:00 End: 11/12/2015 00:00<br>File Format: CSV<br>Time Zone: (GMT) Dublin, Edinburgh, Lisbon, London<br>Document ID : 7-b516ab | | |
| Date/Time | 13/12/2015 06:32 | Clear Event Log | |
| Signed-In User | Anita House (anita.house@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Test Oven – Lab1 (MAC 98:8B:AD:04:1A:CC)<br>Device: Cal Lab - Overlord (MAC 98:8B:AD:02:A2:C6) | | |

| | | | |
|---|---|---|---|
| Date/Time | 13/12/2015 06:32 | Export Data | |
| Signed-In User | Hope Springs (hope.springs@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Freezer 001/A (MAC 98:8B:AD:00:1D:74)<br>Start: 11/12/2015 00:00 End: 12/12/2015 00:00<br>Document ID : 2-d45f41 | | |
| Date/Time | 13/12/2015 04:33 | Add Comments to Data | |
| Signed-In User | Edna Clouds (edna.clouds@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Front Office 32 (MAC 98:8B:AD:02:01:55)<br>Data: 02/12/2015 01:20:18 Pump Temp = 56.4°C Extraction Temp = -10°C<br>Comment: Extraction blockage identified. Maintenance schedule updated. | | |
| Date/Time | 13/12/2015 04:02 | Delete Location | |
| Signed-In User | Edna Clouds (edna.clouds@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Location: Winstanley / California / Test Zone<br>Device: Back Office 32 (MAC 98:8B:AD:02:11:23)<br>Device: Side Office 21 (MAC 98:8B:AD:01:10:04)<br>Device: Big Office 20 (MAC 98:8B:AD:01:11:14)<br>Location: Winstanley / California / Test Zone / Dry box<br>Device: Dry duct 1 (MAC 98:8B:AD:02:07:88)<br>Device: Dry duct 2 (MAC 98:8B:AD:02:09:AB) | | |
| Date/Time | 13/12/2015 03:54 | Export Graph | |
| Signed-In User | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Freezer 001/A (MAC 98:8B:AD:00:1D:74)<br>Start: 11/12/2015 00:00 End: 12/12/2015 00:00<br>Document ID : 2-956621 | | |
| Date/Time | 13/12/2015 03:13 | Archive Device | |
| Signed-In User | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Incubator (MAC 98:8B:AD:02:1A:B4)<br>Device: Freezer 023/Sa (MAC 98:8B:AD:00:20:01)<br>Device: Pre-Chiller 023/Sa (MAC 98:8B:AD:00:24:03) | | |
| Date/Time | 13/12/2015 03:13 | Delete Device | |
| Signed-In User | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Lab Sensor (MAC 98:8B:AD:01:FF:E4) | | |
| Date/Time | 13/12/2015 03:00 | Archive Location | |
| Signed-In User | Edna Clouds (edna.clouds@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Location: Winstanley / California / Test Zone<br>Device: Back Office 32 (MAC 98:8B:AD:02:22:2F)<br>Device: HVAC 100 (MAC 98:8B:AD:01:21:EA) | | |
| Date/Time | 13/12/2015 02:40 | Archive Location | |
| Signed-In User | Edna Clouds (edna.clouds@winstanleyhc.com) | Approved by | Bernard Fusenhauser (Bernard.F@winstanleyhc.com) |
| Comments | Device: Cold Store 4 (MAC 98:8B:AD:00:1D:33)<br>Device: Cold Store 2 (MAC 98:8B:AD:00:20:45)<br>Log Start: 01/12/2015 00:00 Log End: 11/12/2015 00:00<br>Document ID : 4-231d6c | | |

# Standalone 21CFR USB

## Sec. 11.10 Controls for Closed Systems

| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| 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.<br><br>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. | ✓ | EasyLog 21CFR provides an audit trail, detailing user activities. |
| 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. 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. | ✓ | EasyLog 21CFR generates complete copies of all records in both human readable and electronic form - which can be used for inspection, review and copying by the agency |
| c) Protection of records to enable their accurate and ready retrieval throughout the records retention period. | ✓ | EasyLog 21CFR's records are readily retrievable and protected by encryption to ensure their accuracy. |
| d) Limiting system access to authorized individuals. | ✓ | EasyLog 21CFR implements a password protected login procedure. Administrators can set user privileges for each user, and can be can be notified of unsuccesful login attempts via email. |
| 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. | ✓ | EasyLog 21CFR generates an audit trail, detailing all user activities.<br>For more information on what is included in audit trails, please see table 1.<br>EasyLog 21CFR never overwrites any previously saved data or documentation, including audit trails. |
| f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. | ✓ | EasyLog 21CFR is designed to ensure that the user is limited to performing one function at a time, and in the correct order. |
| 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. | ✓ | Yes - please see Sec. 11.10 d). |
| h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | N/A | Not applicable to EasyLog 21CFR. |
| 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. | ✓ ⓘ | This is the user's responsibility. The data logger comes with a Quick Start Guide, and a thorough help file is included within the software. |

| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| 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. |  | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| k) Use of appropriate controls over systems documentation including: | | |
| 1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. |  | This is the user's responsibility. EasyLog 21CFR comes with a Quick Start Guide, and a thorough help file is included within the software. |
| 2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. |  | EasyLog 21CFR provides an audit trail to show changes made to software settings.<br><br>In-house procedures are the user's responsibility. Users need to have their own Standard Operating Procedure. |

## Sec. 11.50 Signature Manifestations

| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| 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; | ✓ | Yes - please see Sec. 11.10 e). |
| 2) The date and time when the signature was executed; and | ✓ | Yes - please see Sec. 11.10 e). |
| 3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. | ✓ | Yes - please see Sec. 11.10 e). |
| b) The items identified in paragraphs a1), a2), and a3) 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). | ✓ | The audit trail EasyLog 21CFR produces is protected by encryption. This can be viewed in the software, or printed out by authorised users. |

## Sec. 11.70 Signature/Record Linking

| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| 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. | ✓ | Yes - please see Sec. 11.10 e). |

# Subpart C - Electronics Signatures

## Sec. 11.100 General Requirements

| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. | ✓ | EasyLog 21CFR users create their own password for their account. Login names cannot be duplicated. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure. |

## Sec. 11.200 Electronic Signature Components and Controls

| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| a) Electronic signatures that are not based upon biometrics shall: | | |
| 1) Employ at least two distinct identification components such as an identification code and password. | ✓ | EasyLog 21CFR uses Login Name, Password and Signature to identify individual users. |
| 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. | ✓ | Each entry on the audit trail in EasyLog 21CFR is identified by two pieces of information - user name and unique user ID. |
| 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. | ✓ | Each entry on the audit trail in EasyLog 21CFR is identified by two pieces of information - user name and unique user ID. |
| 2) Be used only by their genuine owners; and | ✓ | Please see Sec. 11.100 a). |
| 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. | ✓ | Please see Sec. 11.100 a). |
| b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. | N/A | |

## Sec. 11.300 Controls for Identification Codes/Passwords

| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| 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. | ✓ | Please see Sec. 11.100 a). |
| b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | ✓ | Users of EasyLog 21CFR must change their password after an administrator-specified amount of time (from 7 to 999 days). |

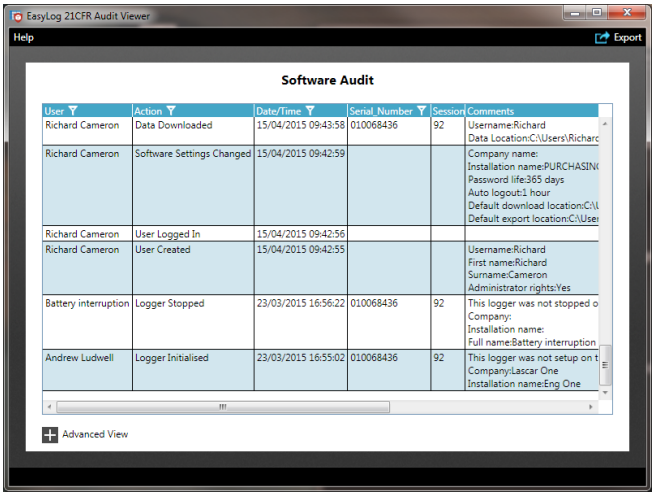
| 21CFR Part 11 requirement | Does EasyLog 21CFR meet this requirement? | Comments |
|---|---|---|
| c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. | ✓ ! | Users can be disabled by an administrator. In the event that a user forgets their password, it can be reset by an administrator. It is the user's responsibility to make sure this is covered in their Standard Operating Procedure. |
| 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. | ✓ | EasyLog 21CFR tracks all login and logout instances in the audit trail.<br><br>Administrators can be notified of unsuccessful login attempts via email. |
| 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. | ✓ ! | This is the user's responsibility. Users need to have their own Standard Operating Procedure |

✓ = Fully Compliant ! = Compliant with user control via SOPs (Standard Operating Procedures

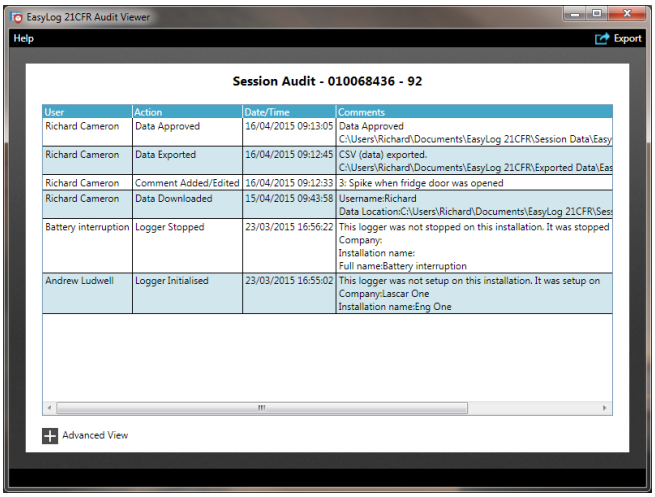
## Table 1 - Audit Trail Entries

| Audit Entries | Software Audit | Session Audit |
|---|---|---|
| User Created | ✓ | |
| User Edited | ✓ | |
| User Disabled | ✓ | |
| User Logged In | ✓ | |
| User Logged Out | ✓ | |
| Failed Log In | ✓ | |
| Users Password Changed | ✓ | |
| Users Password Created | ✓ | |
| Software Settings Changed | ✓ | |
| Users Password Reset | ✓ | |
| Logger Initialised | ✓ | ✓ |
| Logger Stopped | ✓ | ✓ |
| Data Downloaded | ✓ | ✓ |
| Comment Added/Edited | ✓ | ✓ |
| Data Approved | ✓ | ✓ |
| Data Un-Approved | ✓ | ✓ |
| Data Exported | ✓ | ✓ |

## Example Software Audit




## Example Session Audit




## Example Graph with Signatures