21CFR Requirement Checklist

EasyLog 21CFR

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

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

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. 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 unsuccessful 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. For more information on what is included in audit trails, please see table 1. 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).

21CFR Part 11 requirement	Does EasyLog 21CFR meet this requirement?	Comments
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.
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. 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).

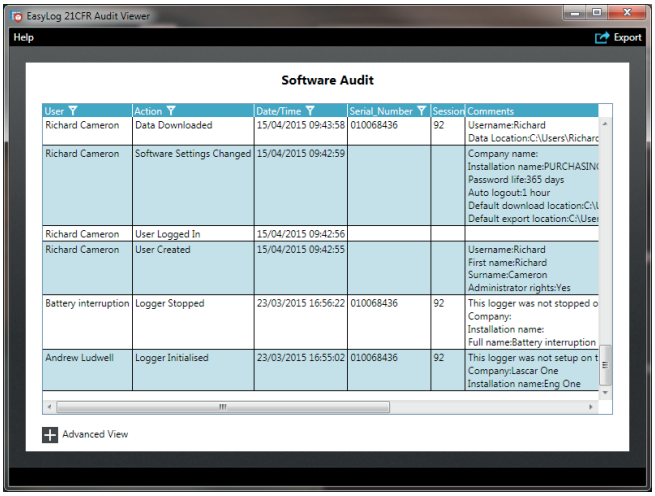
21CFR Part 11 requirement	Does EasyLog 21CFR meet this requirement?	Comments
c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, 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. 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

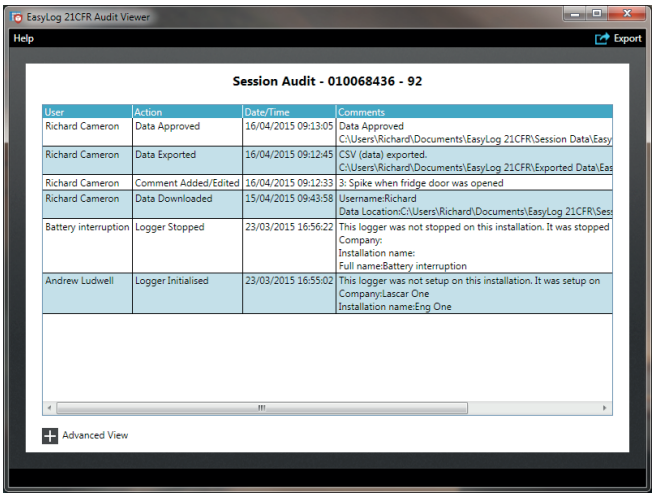
Table 1 - Audit Trail Entries

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