

Complete Compliance with 21 CFR Part 11

CountWire™ System for the LUNA-FX7™



With advancing technology and the subsequent increase in electronic record keeping, the demand for electronic data protection and security is more prevalent. To ensure the accuracy, reliability, authenticity, and consistency of electronic records the United States Food & Drug Administration established Title 21 also known as 21 CFR Part 11, to regulate electronic records and electronic signatures.

In general, Part 11 applies, with some specific exceptions, to drug producers, medical device manufacturers, biotech companies, developers of biologics, CROs and other industries controlled by the FDA. Regulated institutions are required to carry out controls, audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in generating, processing, and storing electronic data.

The 21 CFR Part 11 consists of 3 subparts, General Provisions, Electronic Records, and Electronic Signature. Because the General Provisions subpart includes explanations related to scope, implementation, and definitions; we will focus mainly on the details of subpart B and in this document.

SUBPART A General Provisions	SUBPART B Electronic Records	SUBPART C Electronic Signatures
<p>The scope of the regulations, where and how the regulations should be applied, and provides definitions for key terms used in the regulations.</p>	<p>Requirements for controls of closed and open electronic record-keeping systems, signature manifestations and requirements for signatures and records to be linked.</p>	<p>Three parts: 1) general requirements for electronic signatures, 2) electronic signature components and controls, and 3) controls for identification codes/passwords.</p>
<p>11.1 Scope 11.2 Implementation 11.3 Definitions</p>	<p>11.10 Controls for closed systems 11.30 Controls for open systems 11.50 Signature Manifestations 11.70 Signature record/linking</p>	<p>11.100 General Requirements 11.200 Electronic signature components and controls 11.300 Controls for Identification codes/passwords</p>

CountWire™ System: 21 CFR Part 11 Ready

CountWire™ System Components: Control – Store - Create



The CountWire™ System consists of the CountWire™ Client software installed in PCs, the CountWire™ Data Storage, and the LUNA-FX7™ Automated Cell Counter, connected and controlled under the same network.

The CountWire™ System allows multiple users to remotely access and manage data from multiple LUNA-FX7™ units connected to the network. Working through a PC connected to a network, authorized users may access data from one or more devices, no matter where they may be located. Further, users may approve counting reports on the LUNA-FX7™, without having to move to a PC.

The CountWire™ System completely supports 21 CFR Part 11 compliance, enabling the LUNA-FX7™ Automated Cell Counter to be used in a regulated process. This document provides guidelines on how the CountWire™ System is compliant with 21 CFR Part 11 regulations when it is used as a closed system.

User Management & Access Control

The CountWire™ System establishes two user groups, Administrators and Users with different levels of access and privilege. Within Users, there are further access levels: Creator, Reviewer, and Approver. Users may be organized into groups based upon accessibility and approval lines. The CountWire™ System's user management provides a high degree of flexibility in establishing user roles.

Only authorized administrators and users may access the system with a user ID and password. Administrators, among other roles, establish and manage password related settings and functions such as minimum length, valid period, account locks and invalid login attempt lockouts.

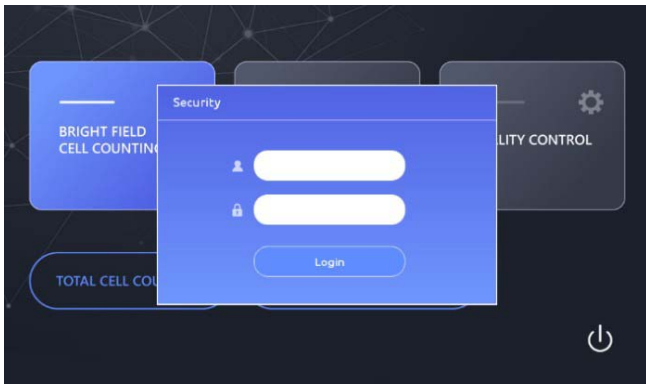
Administrators also are responsible for establishing user and group levels that control accessibility to data.

Data may only be created after an authorized user logs into the system. Upon successful login, the LUNA-FX7™ switches to Security mode.

When operating under Security mode all actions are recorded within the audit trail, time stamped, tagged to user, identified with the instrument name and serial number. Further, only data and counting reports created under Security mode may be forwarded for report approval.

The screenshot shows the CountWire login window. It features the CountWire logo and a shield icon on the left. On the right, there are input fields for 'Storage IP' (192, 168, 0, 39), 'Storage port' (22), 'User ID', and 'Password'. Below these fields are 'LOG IN' and 'SIGN UP' buttons.

The screenshot shows the Password settings configuration window. It includes a 'Password' section with a refresh icon. Below this are settings for 'Minimum length' (8 Characters (8 - 20)), 'Change cycle' (2 Months (1 - 12)), and 'Account lock' (3 Invalid login (3 - 10)). A 'Miscellaneous' section includes 'Auto logout' (10 Minutes (5 - 60)) and 'Self approval' (ON).







Administrator | **Users**



Approver

Reviewer

Creator

Role/Level	What they do
Administrator	 Responsible for system settings, management, and accessibility.
User	Approver  Responsible for final approval of counting reports. Allowed to perform reviewer and creator roles.
	Reviewer  Responsible for reviewing and approving counting reports. Allowed to perform creator role.
	Creator  Responsible for creating counting reports and approving the reports they create.

Modify account ✕

User ID:

Print name:

Group:

Level: Creator Reviewer Approver

Status: ON

Approval

- DEFAULT
- Lab1
 - Approvers
 - lab1_lucy.hildebrant
 - Reviewers
 - lab1_james.kim
 - lab1_miyeon.kim
 - Creators
 - lab1_iam.husher
- Lab2

Electronic Signature

All reports may be digitally signed. The electronic signature information includes the name and User ID of the signer, the date and time of signature execution and meaning (e.g. review or approval) of the signature.

Saves and approvals of the counting data require User ID and password. Each user ID and password must be unique and only one active user ID may be assigned to each person. All signatures are linked to the related electronic records and cannot be removed any record.

The screenshot shows a 'Cell Count Report' interface. A callout box highlights the signature information for three roles: Creator, Reviewer, and Approver. The report itself includes device settings, protocol details, cell counting results, and cell images.

Role	Signature Information
Creator	lab1_lucy.brown Lucy Brown 20 Oct 2020 16:25:30
Reviewer	lab1_emma.kim Emma Kim 20 Oct 2020 17:36:20
Approver	lab1_william.liu William Liu 20 Oct 2020 18:24:55

Audit Trail

All actions and changes are retained in the event log. The event log includes, the Date & Time, User ID, Instrument name, Instrument serial number, and actions taken while logged in. New audit trail values are recorded in addition to old values; and audit trails may not be modified, deleted, or deactivated. Audit trails may be exported or printed for the review.

The screenshot displays the 'Event log' section of the CountWire software. It features a table with columns for Date & Time, User ID, Instrument, Serial No, and Event. The table lists various system events such as logins, logouts, report printing, and instrument settings modifications. At the bottom right, there are buttons for 'PRINT' and 'EXPORT'.

Date & Time	User ID	Instrument	Serial No	Event
20201215 15:24:30	administrator	CountWire		Event log exported
20201215 15:24:56	administrator	CountWire		Event log printed
20201215 15:24:46	administrator	CountWire		Event log printed
20201215 15:24:27	lab1_lucy.brown	lab1	LU7-00-00020	Logout by timeout
20201215 15:23:23	administrator	CountWire		Login successful
20201215 15:14:27	lab1_lucy.brown	CountWire		Login successful
20201215 15:13:30	lab1_lucy.brown	CountWire		Login successful
20201215 15:12:36	lab1_lucy.brown	CountWire		Report printed - Name/LU7-00-00020_20201214140518/LU7-00-00020_20201214140518 - Ch A
20201215 15:06:12	lab1_lucy.brown	lab1	LU7-00-00020	Cell counting completed
20201215 15:04:37	lab1_lucy.brown	CountWire		Report approved - Name/LU7-00-00020_20201214140445
20201215 15:04:12	lab1_lucy.brown	CountWire		Report approved - Name/LU7-00-00020_20201214140413
20201215 15:03:05	lab1_lucy.brown	lab1	LU7-00-00020	Cell counting performed - Protocol name/DEFAULT
20201215 15:01:53	lab1_lucy.brown	CountWire		Login successful
20201215 15:01:49	administrator	CountWire		Login tried
20201215 15:01:25	administrator	CountWire		Logout
20201215 15:01:11	lab1_lucy.brown	lab1	LU7-00-00020	Current setting - Autofocus upon slide insertion/On
20201215 15:01:10	lab1_lucy.brown	lab1	LU7-00-00020	Current setting - Autofocused counting/On
20201215 15:01:09	lab1_lucy.brown	lab1	LU7-00-00020	Current setting - Staining options/Not applicable
20201215 15:01:08	lab1_lucy.brown	lab1	LU7-00-00020	Current setting - Counting chamber area/All
20201215 15:01:08	lab1_lucy.brown	lab1	LU7-00-00020	Current setting - Combine results of selected chambers/On
20201215 15:01:07	lab1_lucy.brown	lab1	LU7-00-00020	Current setting - Slide/3 Ch.
20201215 15:01:06	administrator	CountWire		Instrument setting modified - Cell counting setting modified - lab1/Combine results of selected chambers/Off -> On

Data Safety and Security

The CountWire™ System reliably protects all from deletion, overwriting, alteration, and/or possible accidents. The CountWire™ Data Storage capacity is 4 TB with a mirrored 4 TB of storage to protect the data in the event of physical damage to the system. Deletion or overwriting of data is not allowed in the CountWire™ System. The authenticity of the approved reports is confirmed and displayed by icons. The authenticity of a report is represented by color coded icons.



The original report is in good condition.



The original report may be damaged or forged.

The screenshot displays the CountWire interface. On the left, a table lists data entries with columns for Date, File, Instrument, User ID, Creator, Reviewer, and Approver. The table shows multiple entries for 'lab1' with various dates and file names. On the right, a 'Cell Count Report' preview is shown, including a table of parameters, a 'Cell counting results' section, and two microscopy images. Below the images are buttons for 'Approve', 'Print', and 'Export', and a list of approvals: 'Approved by James O'Connor', 'Approved by Emma Kim', and 'Approved by William Liu'.



-  Approved by *James O'Connor*
-  Approved by *Emma Kim*
-  Approved by *William Liu*

Meeting the Regulatory Requirements of 21 CFR Part 11 with the CountWire™ System

The table below explains how the features and functions of the CountWire™ System connected with the LUNA-FX7™ satisfies the requirements of 21 CFR Part 11.

Important! Please note that the descriptions and explanations we provide represent our interpretations of the 21 CFR Part 11 regulations as the product provider, not representing any government agency.

Part and Description	Comment
Subpart B - Electronic Records	
<i>Controls for Closed Systems</i>	
System Validation	
<p>11.10 (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</p>	<p>Invalid or altered records are recognized by the system by comparing them with the encrypted original records. CountWire™ Client displays the authenticity of the report. All records are read-only and cannot be modified or removed by any user or administrator. A validation guideline for the CountWire™ System is available.</p>
Human Readable Records	
<p>11.10 (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.</p>	<p>The CountWire™ Client software generates human-readable PDF reports that may be printed for inspection, off-line reviews, and duplication by the FDA. Counting reports and audit trails may be exported in PDF format through the CountWire™ Client to a user's PC. Reports may be printed from the PC. From the user's PC, the data may be transferred to USB flash drives or through the network. However, after any data has been exported, Logos Biosystems is not responsible for further data security.</p>
Protection of Records	
<p>11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</p>	<p>All electronic records are backed up in the mirroring storage so that data may be recovered after a possible computer system failure. The CountWire™ Data Storage is up to 4 TB with an additional, mirrored 4 TBs storage. Data cannot be over written. When a user attempts to save data under a previously used file name, the system automatically adds a suffix to the file's name to generate a unique name.</p>
Limiting System Access	
<p>11.10 (d) Limiting system access to authorized individuals.</p>	<p>The CountWire™ limits system access to authorized individuals. Users may access the system only with their own ID and password. The CountWire™ supports assigning 3 levels of users or user groups. A different level of privilege may be assigned to each user or group (Creators, Reviewers, or Approvers). The administrator, at any time, may revoke or reassign the privilege of users and groups. The system automatically logs out users after a period of inactivity. An administrator is able to set the inactivity period (5-60 min).</p>

	<p>The CountWire™ allows password requirements to be established by an administrator that include minimum length (8-20 characters), password change cycle (1-12 months) and lockout after invalid log-in attempts (3-10 times/day). Previously used passwords are not allowed to be used by the same user. Only the administrator may unlock an account. All login attempts, successful or not, are recorded in the system event log.</p>
Audit Trails	
<p>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.</p>	<p>The system automatically records and generates audit trails of all user actions that include the date & time, user ID, instrument name, and the instrument's serial number. New audit trail values are recorded in addition to old values. Audit trails are backed up to the mirror storage and not allowed to be deleted. Audit trails may be exported or printed for review. Audit Trails cannot be modified, deleted, or deactivated.</p>
Operational System Checks	
<p>11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.</p>	<p>The system enforces the sequence of data generation. The CountWire™ restricts user access to specific protocols and counting settings (e.g. slide selection). Users are only allowed to perform the steps their level of privilege grants. All events within the system are ordered and time-stamped within the audit trail.</p>
Authority Checks	
<p>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.</p>	<p>Accessing the CountWire™ software requires a unique user ID and PW in addition to the login information required to access the computer system. The system allows different access control level for the different user levels: creator, reviewer, and approver. A user may only access the system with a valid user ID and password. Users are required to log-in after every inactivity or user-initiated logout. Any changes and modifications to the system by a user are recorded and assigned to their user ID.</p>
Device Checks	
<p>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.</p>	<p>The system checks the validity of the data source. By recognizing instrument names, serial numbers, and IP addresses through proprietary binary communications.</p>
Training	
<p>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.</p>	<p>The organization using the system is responsible for ensuring that users and administrators have the education, training and experience required to perform their tasks. Documents and training are provided only by Logos Biosystems. External maintenance services may only be provided by Logos Biosystems.</p>

Policies for Signatures	
<p>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.</p>	<p>The organization is responsible for developing written policies that ensure the individuals are accountable and responsible for actions initiated under their electronic signatures.</p>
System Documentation	
<p>11.10 (k) (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</p>	<p>Documentation such as the user manual and software update notices are available for the users and administrators. However, controls over the storage and distribution of any documentation are the organization's responsibility.</p>
<p>11.10 (k) (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</p>	<p>Logos Biosystems follows revision and change control procedures and life cycle management procedures for document control. The CountWire™ Client software may be updated by the administrator or users. Only the administrator may update the CountWire™ Data Storage program. All data will remain intact with no loss of data security or traceability after any update. Only creation of reports is allowed. Reports cannot be modified or deleted. All report creations are time-stamped and logged as part of the audit trail.</p>
Controls for Open Systems	
<p>11.30 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.</p>	<p>Logos Biosystems encourages the use of the system as a closed system. If used as an open system, the organization is responsible for ensuring the authenticity, integrity, and, if appropriate, the confidentiality of the system's electronic records.</p>
Signature Manifestations	
Content of a Digital Signature	
<p>11.50 (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; (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.</p>	<p>The CountWire™s digital signatures contain 1) the printed name of the signer; 2) the date and time when the signature was executed; and 3) the meaning (such as creator, reviewer, approver, responsibility, or authorship) of the signature. The CountWire™ allows two roles: an administrator and users. For users there three levels: creator, reviewer, and approver. Only the system administrator can enable and modify the level of the user.</p>

Human Readable Form	
<p>11.50 (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).</p>	<p>All items in the signatures, user ID, printed name, date and time, and meaning are included in the human-readable form, PDF files.</p>
Signature/Record Linking	
<p>11.70 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.</p>	<p>Signatures and approvals require user ID and password. Signatures cannot be excised, copied, or transferred. All electronic signatures are linked to the respective electronic records. Electronic signatures are embedded in the document and encrypted.</p>
Subpart C - Electronic Signatures	
General Requirements	
Uniqueness	
<p>11.100 (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.</p>	<p>Electronic signatures cannot be reused and should be executed for each new electronic record. The organization is responsible for verifying the identity of the individual executing the signature.</p>
Verification of Identity	
<p>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.</p>	<p>Electronic signatures cannot be reused and should be executed for each new electronic record. The organization is responsible for verifying the identity of the individual executing the signature.</p>
Certification of Equivalence	
<p>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.</p>	<p>The organization is responsible for certifying that digital signatures are intended to be legally finding equivalent of handwritten signatures.</p>
<p>11.100 (c) (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.</p>	<p>The organization is responsible for certifying that digital signatures are intended to be legally finding equivalent of handwritten signatures.</p>
<p>11.100 (c) (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.</p>	<p>The organization is responsible for certifying that digital signatures are intended to be legally finding equivalent of handwritten signatures.</p>

Electronic Signature Components and Controls

Signature with Biometrics or Code and Password

11.200 (a) (1)
Employ at least two distinct identification components such as an identification code and password.

CountWire™ employs two distinct identification components: a user ID and password.

11.200 (a) (1) (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.

When an individual executes one or more signings during a continuous period of controlled system access, all electronic signature components must be executed at each signing.

11.200 (a) (1) (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 signature not performed during a single, continuous period of controlled system access requires all signature components.

11.200 (a) (2)
Be used only by their genuine owners.

No two users may have the same user ID/password combination. The organization is responsible for ensuring that proper rules and documentation for executing an electronic signature are in place.

11.200 (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.

The CountWire™ does not provide a proxy signature function. Only the account owner may modify the password and only the administrator can reset the password after proper verification of the user. The enforcement of this policy is the responsibility of the organization that operates the system.

Biometrics Ensure Genuine Owners

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.

CountWire™ does not support biometric signatures.

Controls for Identification Codes/Passwords

Uniqueness of Code/Password

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.

No two individuals may have the same combination of ID and password. User IDs and passwords are required to be unique.

Periodical Check of Issuance (e.g. Password Aging)

11.300 (b)
Ensuring that identification code and password issuances are periodically checked, recalled, or revised.

Passwords will expire and need to be rest after an expiration period (1-12 months) that is set by the administrator.

Loss Management	
<p>11.300 (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.</p>	<p>Only the administrator may reset a password after proper verification of the individual if a user has lost or forgotten a password. In the case of a forgotten user ID is forgotten, a new account should be generated. User IDs are not allowed to be removed or deleted.</p>
Safeguards and Detection of Unauthorized Attempts	
<p>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.</p>	<p>Both components of the electronic signature, ID and password, are executed with each signing. All passwords are stored encrypted and cannot be accessed by any user or administrator. After an administrator-set number (3–10 times/day) consecutive unsuccessful login attempts, a user's account is locked, preventing access. The account remains locked until the administrator resets the password.</p>
Testing of Devices, Cards, etc.	
<p>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.</p>	<p>The CountWire™ does not support devices that bear or generate identification code or password information, such as tokens or cards.</p>
Additional Features and Capabilities which Increase Data Integrity	
<p>The system's administrative software, installed on a PC, may be connected to the network, allowing multiple devices to provide remote access and data management.</p>	<p>The system allows for CountWire™ Client to be installed on a computer, which is physically separated from the location of the LUNA-FX7™ connected over Ethernet or WiFi. This allows for multiple LUNA-FX7™ devices and the software installed PCs to be connected and managed.</p>
<p>After approvals are completed, the data is permanently locked to be read-only to prevent editing.</p>	<p>The system allows for counting reports to be permanently locked to be read-only after results have been approved and signed off.</p>
<p>Data backup and restore procedures to prevent data loss.</p>	<p>The system allows administrative users to perform a backup and restore data. The organization is responsible for establishing and implementing operating procedures to prevent data loss.</p>
<p>Data migration after the system version-up.</p>	<p>All data will remain intact with no loss of data security or traceability after system version updates.</p>
<p>The system must be programmed to automatically log out after an inactivity time set.</p>	<p>The system has an inactive period Auto logout function that is set by an administrator (5–60 min).</p>