Dataworks Development, Inc.
Freezerworks
21 CFR Part 11 Compliance

Standards

Freezerworks was designed and validated using FDA guidelines for software development. Dataworks uses an Agile software development life cycle model. The model is fully described in Dataworks' "Software Development Life Cycle Standard Operating Procedure." The validation portion of that model follows the FDA's "General Principles of Software Validation; Final Guidance for Industry."

FDA Title 21 CFR Part 11 Compliance

Freezerworks includes the following features that will ensure electronic records compliance when used properly:

- A login and password system that forces users to enter a name and valid password to continue

- Expiring passwords

- Masked passwords

- Option to use LDAP and/or SSO for user authentication

- An Audit Trail that is read only and cannot be modified by any user. Every data entry that is changed has an Audit Trail record created that stores the user, the field name, the previous data value, the new data value, the time and date the entry was changed, and the reason for the change. Any tampering of the data, accidental or deliberate, is monitored by the system's automatic and fully secured audit trail, indicating who made a change and when.

Freezerworks does not currently support electronic signatures except in Fulfilling Requisitions.

Freezerworks has undergone a number of compliance audits by current customers, including pharmaceutical companies. Below are a series of questions companies have asked regarding 21 CFR part 11 compliance for which our programs affirmatively meet the requirements.

If you have any additional questions or concerns, please feel free to contact us.

Question Number	Rule Section	Question	Y	N	Comments
1.	§ 11.10(a)	Is there system validation documentation for all program/system software and hardware components?	YES		Electronic copies of all test cases completed by in-house validators are stored indefinitely.
2.	§ 11.10(a)	Does this program/system have the ability to discern invalid or altered records?	YES		The validity of each field and record is checked against user specified configurable standards. Altered records are recorded in the Audit Trail.
3.	§ 11.10(b)	Can the program/system generate accurate and complete records (including administration fields and meta data) in a format (e.g., printouts, screen display, electronic media) that can be read by a human without further manipulation?	YES		Users can configure any viewing screen or any printed report to display any piece of stored data, with the exception of masked User Passwords, in human readable form.
4.	§ 11.10(b)	Can the program/system generate accurate and complete records in a commonly-used electronic format? If yes, identify the electronic format:	YES		ASCII text files – easily read by popular programs -e.g., Microsoft Excel
5.	§ 11.10(c)	Does the program/system protect records in a manner that permits the record to be accurately and readily retrieved for as long as required by the FDA, client's record and retention schedule, and/or client specifications?	YES		There is no expiration to the record protections of the program.
6.	§ 11.10(d)	Does the program/system permit access only to authorized individuals?	YES		Users must enter their unique login and password combination before being allowed access to the program.
6a.		Do non-biometric electronic access codes consist of at least two separate methods for identifying the individual user (e.g., user ID and password)?	YES		See above.

7.	§ 11.10(e)	Is the point at which the data is saved to the recording medium defined and inalterable?	YES	
8.	§ 11.10(e)	Does the program/system include an audit trail capability that records the user name, date and local time (hours, minutes, seconds) of user entries, and actions that create, modify, or delete electronic records, from the time the data is first saved to durable media (e.g., disk, tape)?	YES	The Audit Trail module records and maintains all such data.
9.	§ 11.10(e)	Does the audit trail document changes to a record in a manner that does not obscure or overwrite the information as originally recorded?	YES	New Audit Trail records are created for every new entry, modification, or deletion.
10.	§ 11.10(e)	Does the audit trail include a date and time stamp that allows chronological recording of events without ambiguity (even if the events occur in different time zones), and that records the time of entry based on the time appropriate for the location at which data entry occurs?	YES	Time zone is based on the server where Freezerworks resides, not the location of the user performing the data entry.
11.	§ 11.10(e)	Is the audit trail created independently of the user (i.e., the audit trail is computer-generated and <u>not</u> under the control of the user)?	YES	The user may view and print the Audit Trail, but not modify it manually.
12.	§ 11.10(e)	Is the information in the audit trail protected against being changed by a human user?	YES	See above.
13.	§ 11.10(e)	Is the audit trail retained for as long a period as the record itself is retained?	YES	
14.	§ 11.10(e)	Can the audit trail be readily viewed upon request?	YES	

				ASCII text files
15.	§ 11.10(e)	Can the audit trail be readily copied in an electronic format upon request?	YES	
16.	§ 11.10(e)	Can the audit trail be readily printed upon request?	YES	
17.	§ 11.10(e)	Does the program/system have the capability to control the sequence in which users can perform actions if those actions must be performed in an ordered sequence?	YES	Sequences of events are strictly controlled in any area where data integrity would be compromised if otherwise.
18.	§ 11.10(i)	Were specific education, experience, and training requirements established for the individuals who developed this program/system?	YES	Key developers and managers have over twenty years of database development experience in the area of laboratory inventory and other systems.
19.	§ 11.10(i)	Are systems in use for documenting and verifying compliance with the educational, experiential, and training requirements for developers of this program/system?	YES	Curriculum vitae are stored for each employee. Continuing education is encouraged as needed.
20.	§ 11.10(i)	Have specific education, experience, and training requirements been established for vendors providing this program/system?	YES	
21.	§ 11.10(i)	Are systems in use for documenting and verifying compliance with the educational, experiential, and training requirements for vendors providing this program/system?	YES	
22.	§ 11.10(k)	Is there a complete inventory of all system documentation for users and systems administrators?	YES	

23.	§ 11.10(k)(1)	Is the original version of the documentation, and each subsequent modification, available for review?	YES	
24.	§ 11.10(k)(2)	Is the author, date, and time of the creation of each original document and each modification identified on each document?	YES	
25.	§ 11.10(k)(2)	Are there appropriate revision and change control procedures for maintaining an audit trail that records the date and time of the generation of original system documentation, and of each modification to the system documentation?	YES	See Software Development Life Cycle Standard Operating Procedure
26.	§ 11.30	If the program/system is **open**, (i.e., records reside on, or are transmitted, via a network controlled by a third party such as the internet), are security measures (e.g., document encryption technology) used to ensure the authenticity, integrity, and confidentiality of the records? If yes, identify the technology:	YES	SSL/TLS ENCRYPTION