21 CFR Part 11
Compliance Report

This document explains how the Marathon software products **21CFR DB ™**, **21CFR LE ™**, *and* **21CFR VIEWER™** *address the requirements of the 21 CFR Part 11 set forth ELECTRONIC RECORDS; ELECTRONIC SIGNATURES by the FDA.*

Subpart B—Electronic Records

§ 11.10 Controls for closed systems.	
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	– Marathon Products has determined that, according to the general principles of Software Validation and Verification, the **21CFR DB ™**, **21CFR LE ™**, and **21CFR VIEWER™** software packages satisfy their intended use and user needs. – Recorded files are in binary format, encrypted to 128 or more in a RC4 variant, proprietary to Marathon Products, Inc. Details are not published.
(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.	– Complete, accurate and human readable copies are available on screen, print outs and pdf format (requires pdf printer: Adobe Acrobat or similar). – Complete and accurate electronic records are available in the encrypted database. Additional electronic records can be retrieved as *.edl format from the automatically generated back up or through the use of the export option.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	– On the data logger device, data is held internally in a non-volatile EEPROM memory. – Once downloaded, data is stored into a secure database.
(d) Limiting system access to authorized individuals.	– Individual password protected user accounts.
(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.	– Secure, computer generated, time-stamped audit trails are embedded in the binary history file and located along with the record. – Audit Trails indicate: • Record Creation, Date and Author • Record Append, Date and Author. • Record Revision (Review and Decline), Date, and Author. • Record Approval (Approve and Decline), Date and Author. • Record Import. – Record changes do not obscure previous data. – Records cannot be deleted.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	– The system forces the sequencing of events, e.g. measurement data in the logger memory cannot be deleted without previously saving the data to the database.
(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.	– In addition to individual password protected user accounts, each user can have a unique set of access permissions and privileges customized by the Administrator.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	– Device input and operation status is verified and checked.
(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.	– Procedural. – The administrator sets user profiles and privileges upon evidence of training, according to the company procedures.
(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.	– Procedural. – Awareness of the Electronic Signature liability policy is up to the company procedures.
(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. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	– Marathon Products, Inc provides the software package and pertaining documentation with the correct version and revision identification to facilitate the company change control process.

§ 11.30 Controls for open systems.		
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.	–	The product is targeted to be used in closed systems.

§ 11.50 Signature manifestations.		
(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; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	–	Signed records contain the following information: • Action taken (Creation, Append, Review, Approve, Decline, or Import a record). • Printed Name of the Signer. • Date/Time when the Signature was executed.
(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).	–	The Electronic Signature is located alongside the record and with the same level of encryption. Name (ID), Time-stamp and Meaning are all embedded in the binary format history file.

§ 11.70 Signature/record linking.		
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.	–	The products use Electronic Signatures only.

Subpart C—Electronic Signatures

§ 11.100 General requirements.		
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	–	The products ensure that two user accounts cannot have the same user name. In order to prevent accounts to be reused, user names cannot be deleted, only disabled.
(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.	–	Procedural.
(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. (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. (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.	–	Procedural.

§ 11.200 Electronic signature components and controls.		
(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. (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. (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	–	In order to execute an Electronic Signature, an individual has to provide login name and password at the beginning of the session. For multiple signings during a continuous session, the system automatically validates both components: login and password. This is a result of the ES components are the same login and password used for the controlled system access.
(2) Be used only by their genuine owners; and	–	Users are required to change their passwords at the first login into the system. Passwords are visually encrypted keystrokes.
(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.	–	Users can only change passwords when required by the system password expiration or by the administrator. There is no other way for the user to access his/her password. Unless the users disclose their passwords, it is impossible to tamper with the system.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	–	Not applicable.

§ 11.300 Controls for identification codes/passwords.		
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.	–	User accounts cannot be deleted; all user names are forced to be unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	–	Password expiration is set by the Administrator. User accounts can be disabled but not deleted.
(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.	– – –	Procedural Compromised accounts can be disabled. On loss of password, the administrator may set a new password, which the account holder should then immediately replace by a password of his or her own.
(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.	– –	The products allow setting a minimum length for passwords. Password expiration is set by the Administrator. User accounts can be disabled but not deleted.
(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.	–	Not applicable.