Exhibitor Software and 21 CFR Part 11

MONARCH INSTRUMENT
15 Columbia Drive • Amherst, New Hampshire • 03031-2334
TEL: 603-883-3390 • www.monarchinstrument.com

Subpart B – Electronic Records

Section No. 11.10	Requirement	Responsibility		Related Exhibitor Features	Meets Req.
		Exhibitor	Client		
11.10(a)	**Controls for Closed Systems** Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes		Exhibitor is fully validated and Validation Reference Documentation is available. Monarch Instrument is ISO 9001:2008 certified and has a Quality Management System in accordance with ISO 9001. Log files which include logged process data and audit trail of user activity are in binary encrypted format proprietary to Monarch. Details are not published. Invalid data records are rejected by Exhibitor software and there is no facility to modify the records.	
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.	Yes		DC6000 creates secure unmodifiable electronic records that are encrypted and saved in a format that is accessible only through the Exhibitor software. The system is capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA.	
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	No	Yes	Data is logged to PC media. Archiving and retrieval is the responsibility of the user and should be governed by the user's SOP.	
11.10(d)	Limiting system access to authorized individuals.	Yes	Yes	System Administrator grants access privileges and maintains operator registry.	
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.	Yes	Yes	Each action that could affect the integrity of the Exhibitor software and the data files is logged in an audit trail. This file is composed of data records identifying the type of action performed, the timestamp of this action, the user name associated with this action, and additional information required to understand the action taken. There is no mechanism in place to alter records. Archiving and retrieval is the responsibility of the user and should be governed by the user's SOP. The audit trail is available for review and copying by the FDA.	
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.			Not Applicable	

MONARCH INSTRUMENT
15 Columbia Drive • Amherst, New Hampshire • 03031-2334
TEL: 603-883-3390 • www.monarchinstrument.com

Section No. 11.10	Requirement	Responsibility		Related Exhibitor Features	Meets Req.
		Exhibitor	Client		
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.	Yes	Yes	Exhibitor software requires unique individual ID and password combination for access and operation. A System Administrator grants access privileges and maintains operator registry. The System Administrator creates a new account and assigns passwords and user privileges. Passwords expire as set by the Administrator and System Administrator can disable user accounts. Administrator can disable a user's account automatically after a preset number of consecutive login failures. Whenever an action occurs that requires the user's ID/password combination identification, the user name associated with that ID/password combination and a date and time stamp are written to the secure audit file along with a description of the action.	
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.	Yes	No	System errors and input channel status are alarmed and logged automatically. Various methods to ensure a valid format of operator entered data are available.	
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.	No	Yes	Not Applicable	
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.	No	Yes	Not Applicable	
11.10(k)(1)	Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	No	Yes	Not Applicable	
11.10(k)(2)	Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Yes	Yes	This is a shared responsibility. Monarch Instrument maintains a Quality System based on ISO 9001 certification and will provide, on an ongoing basis, relevant revision and change information to the user. Implementation of changes and maintenance of an audit trail that documents time-sequenced development and modification of systems documentation is the responsibility of the user.	

MONARCH INSTRUMENT
15 Columbia Drive • Amherst, New Hampshire • 03031-2334
TEL: 603-883-3390 • www.monarchinstrument.com

Subpart B – Electronic Records

Section No.	Requirement	Responsibility		Related Exhibitor Features	Meets Req.
		Exhibitor	Client		
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.			Exhibitor software is targeted for use in closed Systems.	
11.50(a)	**Signature manifestation** 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.	Yes	Yes	The Systems Administrator can force all actions to require the use of a unique combination ID/Password (signature) when using the Exhibitor software. Signed records contain printed name (ID), date and time, meaning. Meaning includes signed / authorized plus an operator entered note plus automatically generated action type (e.g. start or stop recording, source of data).	
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)	Yes	Yes	Name (ID), timestamp 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.			Signature manifestation is embedded in the binary format audit file. The appropriate individual(s) can apply either handwritten or an electronic signature generated by means of Exhibitor software for review and approval of records.	

MONARCH INSTRUMENT
15 Columbia Drive • Amherst, New Hampshire • 03031-2334
TEL: 603-883-3390 • www.monarchinstrument.com

Subpart C – Electronic Signatures

Section No.	Requirement	Responsibility		Related Exhibitor Features	Meets Req.
		Exhibitor	Client		
11.100(a)	(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Yes		Exhibitor requires unique individual ID and password combination for access and operation. The System Administrator creates an account and assigns a password.	
11.100(b)	(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.	No	Yes	Not Applicable	
11.100(c)	(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.	No	Yes	Not Applicable	

MONARCH INSTRUMENT
15 Columbia Drive • Amherst, New Hampshire • 03031-2334
TEL: 603-883-3390 • www.monarchinstrument.com

Subpart C – Electronic Signatures

Section No. 11.200	Requirement	Responsibility		Related Exhibitor Features	Meets Req.
		Exhibitor	Client		
11.200(a)	**Electronic signature components and controls** (a) Electronic signatures that are not based upon biometrics shall:				
11.200(a)(1)	(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.	Yes		The System Administrator can set a login timer for user identification. The login timer allows users, after initial identification, to enter only their password if user identification is within the preset time limit. When this option is enabled, the login timer can be set from 1 to 30 minutes. Should the time expire, both user name and password will be required to log back into the system.	
11.200(a)(2)	(2) Be used only by their genuine owners; and	Yes	Yes	Users can change their own passwords and no read access to passwords is provided. It is also possible to have logins time out after a set period of inactivity; to limit the number of login retries before an account is disabled and to force password expiry after a preset number of days. Passwords need to be a minimum length of 5 characters.	
11.200(a)(3)	(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.	Yes	Yes	Users can change their own passwords and no read access to passwords is provided. So, unless one user tells another their password, it is impossible to commit fraud without an audit trail of that fraud being left.	
11.200(b)	(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	

MONARCH INSTRUMENT
15 Columbia Drive • Amherst, New Hampshire • 03031-2334
TEL: 603-883-3390 • www.monarchinstrument.com

Subpart C – Electronic Signatures

Section No. 11.300	Requirement	Responsibility		Related Exhibitor Features	Meets Req.
		Exhibitor	Client		
11.300	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:				
11.300(a)	(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.	Yes	Yes	A System Administrator grants access privileges and maintains operator registry. Exhibitor software requires unique individual ID and password combination for access and operation. The system requires a minimum password length of 5 characters.	
11.300(b)	(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Yes	Yes	It is possible to force password expiry on a preset date. If a user leaves, their account can be deleted.	
11.300(c)	(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.	Yes	Yes	Procedural - Compromised accounts can be disabled. On loss of password, the Administrator may set a new password for an account.	
11.300(d)	(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.	Yes	Yes	It is possible to have logins time out after a set period of inactivity; to limit the number of login retries before an account is disabled; and to force account expiry on a preset date.	
11.300(e)	(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	

AJW 10/02/07
MLK 01/15/13