Implementation of 21CFR11 Features in Micromeritics' Software

Software ID _____

PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A—General Provisions

21CFR11 Section Number and Title	*Requirements of 21CFR11*	*Method of Implementation in Micromeritics' Software*
…	….	
Sec. 11.3 Definitions	The following definitions of terms also apply to this part:	
	(1) **Act** means the Federal Food, Drug, and Cosmetic Act (secs. 201- 903 (21 U.S.C. 321-393)).(2) Agency means the Food and Drug Administration.	Not applicable to MIC software product.
	(3) **Biometrics** means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.	Not implemented in MIC software product; may be implemented at operating system level.
	(4) **Closed system** means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.	MIC software is designed to be used in a closed system.

	(5) **Digital signature** means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.	Not implemented by MIC software. May be implemented at operating system level.
	(6) **Electronic record** means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.	MIC software generates ____ forms of electronic records: .smp files: analysis data .dat files: .rpt files: …..
	(7) **Electronic signature** means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.	Implemented only in the respect that printed and displayed records, and archived electronic records have associated with them the full name identity of the person who generated the data. See Subpart C for details.
	(8) **Handwritten signature** means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.	Not applicable to MIC software.
	(9) **Open system** means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	The MIC software can be used in an open system.

Subpart B—Electronic Records		
Sec. 11.10 Controls for closed systems.	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:	MIC 21CFR11 software provides control and security of electronic records while they are resident in the instrument system. However, it is strongly suggested that these records not be stored on the instrument system, but stored in a more secure environment such as a network, or relegated to the control of an external data management system such as NuGenesis.
	(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	MIC offers supporting information with which to perform validation.
	(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.	MIC's 21CFR11 software provides the capability to product records of analyses (setup parameters, analysis conditions, experimental data) and audit trails in human-readable form on screen or as hard copies. These reports may be embodied, for example, in an Acrobat .pdf file, which also represents a human-readable copy in Portable Data Format.
	(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Records are protected from unauthorized access while on the instrument system computer, however it is strongly suggested that these records be offloaded to a more secure, central environment such as a system network or data management system.
	(d) Limiting system access to authorized individuals.	Access is limited to the MIC instrument software to those individuals who have been assigned logons and passwords. Further security may be implemented at the operating system level to restrict use of the computer on which the instrument system software is executed. A level of authority can be assigned to the logon/password combination so that once logged on to the MIC instrument system, only certain operations can be achieved.
	(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.	An audit trail having attributes as described in 21CFR11 Subpart B, Section 11.10 (e) is maintained.

	(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	
	(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.	Two levels of control are provided in the MIC 21CFR11 software to assure that only authorized individuals can use the system. The first, a unique logon/password combination limits access to the program. Second, a level of authority is assigned by the system administrator to each logon/password, which limits the user to a certain range of operations within the software.
	(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	
	(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.	
	(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.	
	(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.	

Sec.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 Sec. 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.	
Sec. 11.50 Signature manifestations.	(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	
	The printed name of the signer; The date and time when the signature was executed; and The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	
	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).	
Sec. 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.	

Subpart C—Electronic Signatures		
Sec. 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. (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. (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.	
Sec. 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.	
	(2) Be used only by their genuine owners; and	
	(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.	
	(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owner	
Sec. 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.	
	(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	

	(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.	
	(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.	
	(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.	

Note that the FDA has stated that the list of system controls is not intended to be all inclusive of what may be needed for a given electronic records system, and that some controls may not be necessary in all types of systems. The wording is intended to clarify which controls are generally applicable and which are germane to certain types of systems depending upon their intended use. For example, operational checks to enforce permitted sequencing of events would not be appropriate to systems in which proper sequencing was not relevant to the events being recorded. Examples of system controls that would be applicable in all cases include validation and protection of records to ensure that records remain accurate and retrievable throughout their retention period.