AIR. NOTHING ELSE.

VALIDATION SUMMARY

MAS-100 Atmos® microbial compressed gas sampler

The life science business of Merck KGaA, Darmstadt, Germany
operates as MilliporeSigma in the US and Canada.

Millipore®

21 CFR PART 11 CONTROLS

An assessment of the 21CFR part 11 compliance was made by an external company specialized in computerized system validation.

This table outlines the requirements of 21 CFR part 11 and the method of compliance utilized by MAS-100 Atmos® instrument (local user interface (UI) and MAS-100 Atmos® application software. It is a Browser-based User Interface accessible with a web-browser when a computer is connected to the instrument by means of a USB-C (instrument side) to USB-A (computer side) cable.

In this document, only electronics records are considered as MAS-100 Atmos® applications software doesn't manage electronic signatures.

The compliance table is built according to the following rules:

- In the first column, preceded by its reference in the 21CFR11 regulation, the textual repetition of the requirement stated by the FDA,
- In the second column, the mode of response to this requirement:
  - 'P' if it must be "Proceeded" by the company (end user),
  - 'S' if the System (MAS-100 Atmos®) must ensure it,
- In the third column, the synthetic interpretation of this requirement,
- In the fourth column, the result of test stating if it is "Passed" or "Failed", N/A is used when requirement is not applicable to the application software.

REQUIREMENT 21CFR PART 11	MODE OF RESPONSE	SYNTHETIC INTERPRETATION	TEST STATUS
B-11.10.a - Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	P and S	The system should be validated for its ability to detect invalid or corrupted records GMP recommendations were followed for validation and qualification of product and equipment. Evidence can be provided during an audit, thus answering to the "P" part of the requirement	**Passed**
B-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	S	Records must be available: • on the screen, • or in paper form, • or in electronic form via an export for the FDA auditor who only has the most common office automation tools on his computer. The FDA accepts records in PDF format	**Passed**
B-11.10.c - Protection of records to enable their accurate and ready retrieval throughout the records retention period	P and S	Recordings must be protected for the legal retention period	**Passed**
B-11.10.d - Limiting system access to authorized individuals	P and S	The system must be protected against access by unauthorized persons	**Passed**
B-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	S	This point specifies that there must be a timestamp of the data as well as an audit trail on all the actions taken by the users influencing the recorded data An audit trail is a record of all operations performed in the database The system must include a secure audit trail function of each GMP record and user actions. This audit trail must be kept for as long as the records to which it relates It must be available to be inspected or outsourced for the FDA agency	**Passed**

Requirement 21CFR part 11	Mode of response	Synthetic interpretation	Test status
B-11.10.f - Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate	P and S	The system must be able to control, when appropriate, the respect of a sequence of steps or operations (Workflow)	**Passed**
B-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 and S	The company must be able to control authorized interventions on the recordings (creation, modification, deletion). Direct access to stored data must be controlled as well as direct interventions on the supervised process	**Passed**
B-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 and S	This point is to secure user command actions step by step (obligation to go through certain steps) during the supervision of a process (alarm acknowledgment, process start, correction of parameters, launch of end report lot,....). Each action must be able to be carried out by the only user(s) authorized to carry it out. Some of these actions must even be checked or validated by another person who is himself authorized to do so, all of which must be traced in an audit trail (see B-11.10.e) On the other hand, it is necessary to record unsuccessful access attempts by an unauthorized user	**Passed**
B-11.10.i - Determination that persons who develop, maintain, or use electronic record systems have the education, training, and experience to perform their assigned tasks	P	People who develop and maintain or use the system must have the initial training, continuous training and experience necessary to perform their tasks	N/A (Out of assessment scope)
B-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 and S	The company should establish written policies and obtain adherence to hold individuals responsible and accountable for actions taken under their electronic signature in order to discourage signature tampering	
B-11.10.k - Use of appropriate controls over systems documentation including:	/	System documentation should be checked	

Requirement 21CFR part 11	Mode of response	Synthetic interpretation	Test status
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance	P	Distribution and access to system documentation should be subject to appropriate controls	
(2) - Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation	P	The development and modification of system documentation is conducted according to review and change control procedures which include an audit trail	N/A (Out of assessment scope)
B-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.	S	Access to open systems must include additional measures such as encryption or digital signing	N/A (Not an open system)
B-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; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature	S	Electronically signed records must contain the signatory's legal or full name, date and time and meaning of the signature in clear text on all visible forms of the record	N/A (No electronic signature)

Requirement 21CFR part 11	Mode of response	Synthetic interpretation	Test status
B-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)	S	Data from 11.50.a. must be treated as part of the record and be presented in all legible forms of the record	
B-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	S	The signature / registration link is impossible to distend by any common means	N/A (No electronic signature)
C-11.100 a - Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	S	A signature must be: • personal, • unique for each person in each system at a given time, • not reusable • not reassignable	
C-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	Verification of the identity of electronic signature users	

Requirement 21CFR part 11	Mode of response	Synthetic interpretation	Test status
C-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. (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	P	The commitment of the users and administrator is reaffirmed in the case of the implementation of an electronic signature which must be recognized by the user as the equivalent of his handwritten signature in a letter (postal) addressed to the FDA	

Requirement 21CFR part 11	Mode of response	Synthetic interpretation	Test status
C-11.200 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	S	For non-biometric signatures, the system must use at least two distinct means of identification, such as an identifier code and a password, to sign electronically. When an individual performs a series of signatures during a continuous period of controlled access to the system, the system may allow that individual to sign with only one component of their electronic signature, provided that the first signature is performed using all components of the electronic signature The level of security must be such that if a signature is made by a person who does not hold this signature, this necessarily means that the holder has communicated his password to someone The company must guarantee through the system the identity of the people able to sign electronically	N/A (No electronic signature)
C-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	P and S	The system must be designed to ensure that electronic signatures based on biometrics cannot be used by anyone other than their owner	
C-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:	/		

Requirement 21CFR part 11	Mode of response	Synthetic interpretation	Test status
C-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	S	The system must be able to maintain the uniqueness of each username/password combination.	N/A (No electronic signature)
C-11.300 b - Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)	P and S	The management of passwords linked to the signature must respect the criteria of complexity, lifespan, reset, of the customer's procedure	
C-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 and S	The system must provide the possibility of permanently or temporarily deactivating the identification process in place (card or token), in the event of loss. The system must provide the possibility of providing a replacement identification method (card or token) The system administrator can revoke a signature	
C-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	S	The system must be able to detect and trace attempts to use unauthorized electronic signatures	
C-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	The equipment used to generate identification codes or passwords must be tested periodically	

www.sigmaaldrich.com