21 CFR Part 11 – Electronic Records; Electronic Signatures

Moxi V – Firmware version 2.12 Compliance Statement

Section	Description	Rule Overview	Moxi V Compliance
11.3	**Definitions**		
11.3 (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.	Closed System definition	The Moxi V is a self-contained system with its own operating system (OS). There's no need for an external system (e.g. laptop) to control it and there's no networking connections to allow unauthorized external access. System and data access is entirely controlled by the system interface, via the user login and roles/privileges functionality. As such, the Moxi V qualifies as a closed system.
11.10	**Controls for Closed Systems**		
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	System Validation	The Moxi V firmware is validated internally to ensure intended function, performance, and compliance to the 21 CFR Part 11 standard. Checksums are used to verify data is valid and hasn't been altered.
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.	Human readable records / Data Access	Every test saved, as well as any data modification event, on the system results in the generation of a unique image (BMP) file of the result output. The BMP image contains the full data display, results/values, and the latest signature event. The image files are implemented to ensure easy inspection of data (without the need for the system or external software) in a manner that can't be readily modified. Data is also stored separately in the industry-standard flow cytometry standard (FCS 3.1) format. Within that FCS data file, a log of all signature events to the file is recorded, including tracking all changes to gate locations. The FCS data adds the ability to inspect data using any industry-standard FCS compliant

			software package. The FCS output can also be displayed on the system to regenerate the original data.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Data integrity	Access to data files is restricted on the Moxi V system by unique user logins and associated user privileges. Data integrity is ensured by the use of checksums. Once an authorized user has backed up data from the system, it is incumbent on the company to ensure proper storage and security measures for the external data backup.
11.10 (d)	Limiting system access to authorized individuals.	Controlled User Access	Once the "Secure Mode" (21 CFR Part 11) of the system is enabled, all access to the system is strictly controlled by unique user ID and passwords. The system provides an "Idle Shutdown Timer" global setting that administrators can set to specify the automatic logout time (5, 15, 30, 60, or 120 minutes) for a user during a period of inactivity. This provides added protection to help ensure an unattended unit is properly secured.

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.	Audit trails	The Moxi V firmware provides detailed audit trails. At the data/file level, all actions are recorded with each file in the FCS file with the signature information as well as gate location information for gating changes. And, each action, is recorded with an image (BMP) representation of the current data output values, the action that was taken, and the electronic signature of the user that performed the action. At a system level, notable events are logged in a system event log, including
			• Logins
			  ○ Sign-in
			  ○ Sign-out
			  ○ Failed login event
			• User Administration
			  ○ Add a user
			  ○ Edit user (modify a user)
			• Password Change
			• File checksum failure
			• USB connect events
			• Test/Data
			  ○ Creation
			  ○ Modification with Approval
			  ○ Deletion
			• System Power-on
			• System Power-down.
			System event logs are provided as .csv files, accessible only by administrators, in the

			/User/admin folder (after connecting the system as a USB disk). Following copying of the files from the system, companies are responsible for secure storage of the files.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational System Check	Permitted actions are tied to established user roles, assigned to each user ID. Administrators are required to assign every user a role on initial setup of that user, thereby establishing the approved actions for that user.
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.	Authority checks	All access to the system is controlled by unique user ID's and passwords. Users are made aware that entering user ID and passwords (or just passwords) constitutes an electronic signing of the action. Ordinary users are limited to generating signed data but can't modify, delete, or copy the data. Reviewers' have expanded privileges to examine and modify data. Administrators are the only group that can copy data from the system, add users, and alter user privileges.
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.	Device checks	The system implements file checksums to ensure the accuracy/validity of all generated data.
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.	Training	The full functionality of the system firmware is detailed in the system User Guide. ORFLO can offer high-level guidance and training in the user of the firmware. Ultimately, it is the responsibility of the customer to leverage the documentation and support resources to ensure their users are properly trained.
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.	Electronic signature validity	The system emphasizes that the use of a user ID and password entry constitutes a legal signing of actions. More detailed written policies and education would be the responsibility of the customer.
11.10 (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.	Document Revision Control	With the v2.12 (21 CFR, Part 11) release, system User Guides are revision controlled to match the firmware release. All changes to the guide are itemized/logged (audit trail) in a revision tracking document. The process involves verifying all system changes with the development team and dual signature approval of the changes.
11.30	**Controls for open systems.**		N/A - The Moxi V is a closed system.
11.50	**Signature manifestations**		
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;	Signature components	For every signature event, the full name of the signer, date/time of signature, user role, and event type is recorded and logged.

	(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.		
11.50(a)	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).	Signature tracking	Administrators can access and backup the full signature/event audit trail for the system. For signature actions associated with specific data files, a human-readable BMP is generated with the relevant data statistics and manifestation of the signature components.
11.70	**Signature/record linking**		
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.	Signature/ record links	Electronic signatures are included in checksum-protected FCS data as well as in the data images generated for every test/action, creating a permanent link between the records that can't be altered by ordinary means.
Subpart C	**Electronic Signatures**		
11.100	**General requirements**		
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Signature uniqueness	The system ensures that all user ID's are unique so that the corresponding electronic signatures are also unique.
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.	Identity Verification	It is the customer's responsibility to ensure the identity of any individual that is assigned a user ID. The system limits the creation of users (and associated signatures) to Administrators so that a select group of trained individuals is responsible for generating users.
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.	Certification of electronic signature as valid/binding	The system has language to indicate to the user that a user ID / password entry is tantamount to a legal signature. However, ultimately, it is the responsibility of the customer to provide the certification.
11.200	**Electronic signature components and controls**		

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.	Signature implementation requirements	The Moxi V firmware uses two components for signatures: user IDs and passwords. During a given session, the initial action (e.g. File Save) taken by a user, requires both components. Following that initial action, during an active session (no logout, no power-off, no sleep of the system), users are required to just enter passwords for each action. The system does not allow any others, even Administrators, to sign on behalf of another user.
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.	Biometrics	N/A
11.300	**Controls for identification codes/passwords**		
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.	Login uniqueness	The system enforces uniqueness of user ID's so that no two users have identical ones.
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).	Password aging	The Moxi V firmware implements a global setting ("Password Expiration") that allows the Administrator user(s) to specify a password expiration period. Users are required to update passwords based on that setting.
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.	Account inactivation	The system provides the capability for administrator users to delete other users, change passwords, or change user roles.
11.300 (d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in	Password/Login safeguards	The system specifically logs any failed login attempts in the system log.

	an immediate and urgent manner any attempts at their unauthorized use to the system		
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.	Token/Cards	N/A – The Moxi V does not use external tokens or cards. The system firmware, under administrator access, is used to generate and change passwords. Testing of that function is performed for each firmware release by ORFLO.

Document Revision History

Document #	Revision #	Reason
MXV.SYS.006	1.0	Initial release
MXV.SYS.006	1.01	Removal of Gemini Bio branding