21 CFR Part 11 Statement

MACSQuantify™ Software (version 3.0 or higher for MACSQuant® Analyzers, or 3.1 or higher for MACSQuant Tyto® Cell Sorter) with 21 CFR Part 11 module enables the compliance with 21 CFR Part 11 guidelines.

Section		Summary	Features
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 MACSQuantify Software is designed by Miltenyi Biotec to ensure accurate, reliable and intended performance of the MACSQuant System. IQ/OQ procedures can be put in place to ensure operational readiness for the proper functioning of the MACSQuant Instrument. The acquired measurement results (for MACSQuant Analyzer) and the exported electronic records (for MACSQuant Analyzer and MACSQuant Tyto Cell Sorter) are created with a check sum to allow identification of the original 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.	Record generation and copying	The MACSQuantify Software allows the operator the possibility to store and export the measurement results and all relevant analysis parameters in a human readable format. A data Audit Trail containing the measurement results can be exported in an archivable PDF/A standard to comply with 21 CFR Part 11 regulations. A report containing the analysis layout and information about the data files used for the analysis can also be exported to PDF using the PDF/A standard. Reports can be printed for inspection and offline review.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Record protection	All reports are exported together with a checksum to allow the detection of tampering. Security measures for storage of these reports lies within the responsibility of the operating company.
11.10 (d)	Limiting system access to authorized individuals.	Access limitation	The MACSQuantify Software requires all users to log in for system access. Each user has a defined role, including access rights. Roles are assigned within the User Management. Only active users can log in and access the software with a valid and unique user ID and password.

Section		Summary	Features
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	Time-stamped audit trails are recorded for all instrument actions performed by the user (such as calibration and compensation), as well as for all file creation, storage, and transfer activities. Entries for User Management actions are also generated. Date and time changes can only be made by an authorized user and are recorded in the audit trail. Audit trails can be exported in PDF/A format. Creation and signing the analysis report also creates an audit trail report entry. Reports cannot be overwritten.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational system checks	Specific software functions (such as daily instrument calibration) ensure that the instrument operates within its specified parameters.
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	The MACSQuantify Software ensures that users have the proper authority to carry out particular functions based on their roles and access privileges. It is the responsibility of the operating company to ensure that each user name can be traced to a real individual and to ensure correct assignment of roles.
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/terminal checks	The MACSQuantify Software applies checks to allow only valid information to be entered into the appropriate fields. All mqd and FCS data files are checked to ensure a valid data input source. A checksum is applied to acquired mqd data files (not on MACSQuant Tyto Cell Sorter).
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 and user accountability	Miltenyi Biotec developers are fully and continuously trained. Miltenyi Biotec provides MACSQuantify Software user trainings. The operating company is responsible for training on their SOPs in regard to electronic records and electronic signatures. Miltenyi Biotec does support the installation of these SOPs in relation to MACSQuantify Software.
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.		Responsibility of the operating company.
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.	System Document Control	A release-specific software manual is distributed together with the MACSQuantify Software. MACSQuantify Software development is governed by a design and change control process that ensures the creation and tracking of relevant documents.
11.30	**Controls for open systems**		**Not applicable. The MACSQuant Instruments operate as closed system.**

Section		Summary	Features
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; (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.	Signature manifestations	The User Management of the MACSQuantify Software ensures that all user IDs are unique. (1) The system verifies the user credentials before creating an analysis report (the user is required to re-enter his/her user ID and password). The report contains the user ID (2) The date & time of the creation of the analysis report is printed within the report (3) The system requires the user to enter a reason for creating an analysis report. The reason is printed within the report.
11.50 (b)	The items identified in paragraph (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 eletronic record (such as electronic display or printout).		The electronic records generated by MACSQuantify Software are date and time-stamped, and signed by the author. Check sums are available to detect modifications of signed records. Refer to 11.10 (c).
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/record linking	The signature is integrated into the record analysis report and can therefore not be excised, transferred or copied.
11.100	**Electronic Signatures**		
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by or reassigned to anyone else.	Uniqueness of electronic signatures	The MACSQuantify Software User Management ensures that all user IDs are unique. Therefore, all electronic signatures are unique.
11.100 (b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individuals electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Verification of identity	It is the responsibility of the operating company to ensure the identity of the individual at the time of adding the user to the MACSQuantify Software User Management.
11.100 (c)	Certify electronic signatures are equivalent to handwritten signatures and submit to FDA.	Certification	Responsibility of the operating company.
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.	Controls for electronic signatures	MACSQuantify Software requires the entry of the username and password for each signature action. In order for a user to have access to a signature action, the user must have a User ID in the User Management of MACSQuantify and must be logged in with user ID and password.
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.		Not applicable

Section		Summary	Features
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.	Uniqueness of ID/ password	MACSQuantify Software user management ensures uniqueness. In addition to that, the operating company has to ensure the User ID and password used within the LDAP system are unique.
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 MACSQuantify Software provides periodic password expiration and account lockout after multiple authentication failures. In addition, password length, complexity and reuse restrictions are implemented by the system. Criteria can be configured by an authorized user and can be customized by the operating company. If the software is configured to use a customer's LDAP system for user authentication, it is the responsibility of the operating company to ensure that features such as password aging, etc. are implemented.
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.	Lost ID/password management	The MACSQuantify Software allows the administrator to manage user profiles, including user IDs and passwords. Both user management and LDAP setup support local user deactivation. Proper loss management procedures are the responsibility of the operating company.
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.	Controls to prevent unauthorized credential use	The operating system of MACSQuant Instrument locks the screen after an inactive period to prevent unauthorized use. The length of the inactive period before the screen is locked can be set individually by the operating company. The MACSQuantify Software provides account lockout after consecutive authentication failures; the number of consecutive failures can be set by an authorized user. Other transaction safeguards, such as monitoring of locked accounts, etc., are the responsibility of the operating company.
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.	Periodic testing of ID/ password generation	Responsibility of the operating company.

Miltenyi Biotec

Miltenyi Biotec B.V. & Co. KG | Friedrich-Ebert-Straße 68 | 51429 Bergisch Gladbach | Germany | Phone +49 2204 8306-0 | Fax +49 2204 85197
macsde@miltenyi.com | **www.miltenyibiotec.com**

Miltenyi Biotec provides products and services worldwide. Visit **www.miltenyibiotec.com/local** to find your nearest Miltenyi Biotec contact.

130-134-238.02