MALVERN MASTERSIZER 3000
21 CFR Part 11 Gap Analysis

Table of Contents

1.1 Regulatory Requirements for e-record systems (21 CFR Part11)

21CFR11 Reference	Possible Interpretation	Is this met?	Comment
§ 11.10 (b)	The computerized system must either support the viewing of e-records or the generation of valid paper copies. The computerized system should provide viewing & printing capabilities for all relevant e-records.	Y	Result records can be viewed in the Mastersizer 3000 software or printed for viewing later.
§ 11.10 (b)	The computerized system should allow for the export of e-records to portable file formats, preferably automatically.	Y	A data export template can be set up in the Mastersizer 3000 application to export any set of parameters. This can then be used to export to a text file either manually (after a measurement is completed) or automatically during the measurement process.
§ 11.10 (c)	If the retention strategy does not include keeping the e-records in the originating system, the computerized system should have implemented a mechanism to archive e-records in a standard file format.	N	Malvern does not provide an archiving system. This requirement needs to be met by the user's IT department.
§ 11.10 (c)	Preferably e-records should be archived to write-protected media (Write-once Read-many media like WORM tape media or optical media) or archiving solutions with WORM type safeguards should be used.	N	Malvern does not provide an archiving system. This requirement needs to be met by the user's IT department.
§ 11.10 (c)	If automated archiving is put into practice, transaction safeguards should prevent the e-records in the source system from deletion until confirmation that they have been successfully archived.	N	Malvern does not provide an archiving system. This requirement needs to be met through the configuration of the Windows security system. This will need to be done by the user's IT department.

21 CFR Part 11 Gap Analysis

21CFR11 Reference	Possible Interpretation	Is this met?	Comment
§ 11.10 (d)	If the computerized system is accessed through workstations which bear more than one application, the application must have its own security layer (*e.g. application specific User ID / password versus workstation "power-up" User Id & password*).	N	The system security layer uses Windows ID, but roles can be assigned to specific Windows users using the Malvern Access Configurator (MAC) application.
§ 11.10 (d)	Ensure that the computerized system has a security mechanism that uses at least two distinct identification components or biometrics.	Y	The Mastersizer 3000 software security layer uses the Windows security system to control software access. This requirement therefore needs to be configured by the local IT department.
§ 11.10 (d)	The CS must allow for the use of individual accounts, shared accounts for access levels other than read are not acceptable.	Y	Individual accounts can be set up using the Malvern Access Configurator (MAC) application.
§ 11.10 (d)	The computerized system should provide a mechanism to lock out/ interrupt access of any user after a configurable period of non-attendance/ non-interaction with the system.	Y	The Mastersizer 3000 software security layer uses the Windows security system to control software access. This requirement therefore needs to be configured by the local IT department.
§ 11.10 (d)	The implementation of the lock out process should be well investigated in regard to safety needs. Access to safety relevant functions & operations must always be possible and should be given priority.	Y	No safety issues associated with the lock-out of the Mastersizer 3000 software.
§ 11.10 (d)	If technically possible, passwords must be stored in the computerized system in an encrypted form.	Y	The Mastersizer 3000 software security layer uses the Windows security system to control software access. This requirement therefore needs to be configured by the local IT department.
§ 11.10 (d)	When password entry fields are shown on the screen, password entries must be obscured (e.g. "*********").	Y	The Mastersizer 3000 software security layer uses the Windows security system to control software access. This requirement therefore needs to be configured by the local IT department.
§ 11.10 (d)	The system should allow for quality passwords (at least 8 alphanumeric characters) and enforce their use.	Y	The Mastersizer 3000 software security layer uses the Windows security system to control software access. This requirement therefore needs to be configured by the local IT department.
§ 11.10 (e)	If the computerized system provides for secured, computer-generated audit trails for e-records, they must be enabled.	Y	Audit trails provided for all record creation and system operations within the Mastersizer 3000 application.
§ 11.10 (e)	Whenever traceability must be guaranteed for records which : - are subject to frequent manipulations or - could become modified and have a direct impact on drug product quality and safety, check that the computerized system has the ability to generate secured audit trails.	Y	Audit trails provided for all record creation and system operations within the Mastersizer 3000 application.

21 CFR Part 11 Gap Analysis

21CFR11 Reference	Possible Interpretation	Is this met?	Comment
§ 11.10 (e)	Computer generated audit trails should contain information about: - WHO performed an activity - date and time of its execution (WHEN) - WHAT was changed/ done - the reason for the activity (WHY) if appropriate	Y	Audit trails provided for record creation and system operations. These provide time-stamped entries for auditable actions. The user's name is automatically recorded, as is the action which was carried out. A reason for change is requested for key record creation / editing / deletion actions.
§ 11.10 (e)	Audit trails must be built using a unique identifier to trace "WHO did it" (preferably the unique User ID).	Y	The audit trails not only log the name of the user who carried out an action, but also log the unique Windows security identifies for the user.
§ 11.10 (e)	Computer generated audit trails should at least record the hour and minute and must be as precise as required by the business process.	Y	Audit trails log the time for each action, using the standard Windows format. This provides a unique time stamp which is recognizable within any time zone.
§ 11.10 (e)	The server time should be used for the generation of time stamps.	Y	Audit time stamps rely on the system time on the computer which is running the Mastersizer 3000 application.
§ 11.10 (e)	Time & date settings should be subject to rigorous control, to ensure the accuracy of time stamps. The computerized system should provide the ability to restrict access to time settings.	Y	Audit time stamps rely on the system time on the computer which is running the Mastersizer 3000 application. The ability to change the reported time therefore needs to be secured within the Windows operating system.
§ 11.10 (e)	The computerized system should have a mechanism to prevent changes to e-records that obscure or destroy the original recorded information.	Y	Original measurement data is stored and cannot be modified. Recalculations based on this data create a new measurement record. This process is audited.
§ 11.10 (e)	If audit trail information is not part of the record itself, the computerized system must implement mechanisms to establish a secured link between audit trail & the respective record.	Y	Both a system audit trail and a record based audit trail are present. The record audit is directly associated with the record being audited.
§ 11.10 (e)	The ability to change computer generated audit trails must be restricted to a minimum number of individuals and to duly authorize personal. Audit trails should only be changeable by the following role: Administrator	N	Audit trails cannot be changed from within the application.
§ 11.10 (e)	The computerized system should provide viewing & printing capabilities for all relevant audit trails.	Y	Audit trails can be viewed from within the application. In addition, the audit trail files are stored in a human-readable format external to the program, and can therefore be viewed and printed using other Windows applications.

21 CFR Part 11 Gap Analysis

21CFR11 Reference	Possible Interpretation	Is this met?	Comment
§ 11.10 (f)	If the adherence to certain sequences is critical to the proper conduct of the process, the computerized system should support operational system checks to enforce the execution of operations according to the predefined order.	Y	The Mastersizer 3000's measurement SOPs enforce a robust record creation sequence.
§ 11.10 (g)	The computerized system should apply authority checks to ensure that only authorized individuals can: - make use of system functions & features - electronically sign a record, - create, modify, inactivate/ logically delete, delete records, - access input and/ or output devices, - perform operations at hand. Authority checks should be implemented by role based access.	Y	Different user roles can be created within the Malvern Access Configurator (MAC) application. These are based on the Windows users and groups available on the computer system running the Mastersizer 3000 software. Using these roles, access to key record creation, editing and deletion functions can be controlled.
§ 11.10 (g)	The computerized system should enforce record specific access rights (e.g. only the originator of a record is allowed to modify it) whenever the business process asks for such controls. This can be achieved by maintaining a list of those records, an individual is allowed to modify/ sign. Before access to a record is provided for an individual, the computerized system should check if this record is part of the individual's list.	N	Modification of records can be controlled using the Mastersizer 3000 security system. In this way, specific users can be blocked from modifying records. However, there is no specific mechanism for allowing the original record creator to make changes.
§ 11.10 (g)	The computerized system should provide mechanisms that prevent users - except those authorized to do so - from having access other than "read" to records. If the computerized system lacks such controls, computer-generated audit trails must be implemented.	Y	Record creation, editing and deletion can be controlled using the Mastersizer 3000 application's security system. An audit trail is also provided to log key system and record actions.
§ 11.10 (h)	In cases where the physical identity of a HW item/ device/ equipment is relevant, the computerized system should check the identity of such devices.	Y	The serial numbers of Mastersizer 3000 optical bench and attached dispersion accessories are recorded within each measurement record.
§ 11.30	Operation within an open environment.	N	Operation in an open environment is not supported by the Mastersizer 3000 application.

1.2 Regulatory Requirements for e-signature systems (21 CFR Part11):

21CFR11 Reference	Possible Interpretation	Is this met?	Comment
§ 11.50 (a)	Ensure that all users are uniquely identifiable in the computerized system.	Y	The Mastersizer 3000 software security layer uses the Windows security system to control software access. The users name and Windows security ID are logged with any signature applied to a record.
§ 11.50 (a)	The computerized system must record / link: • the unique identifier of the person executing the signature • the date & time of the signature • the meaning of a signature (e.g. approval; review).	Y	The user ID is taken from Windows login details. When signature is requested, the user is prompted to authenticate and the time & time is recorded. Users can provide a reason for a signature as a free text string. Authorized users (set up within the Malvern Access Controller application) can lock a record following the application of their signature.
§ 11.50 (a)	The computerized system should allow for pre-programming of signature meanings, if this makes a good business sense, e.g. in case of predictable and/ or recurrent signature meanings.	N	This function is not available within the Mastersizer 3000 software.
§ 11.50 (a)	Where pre-programming of meanings for signatures appears to be not useful, implement free text comments associated with the signature.	Y	Users can add a reason for signing as a free text field.
§ 11.50 (b)	Whenever a signed record is required to be used for GxP purposes, ensure that the full name of the signer, date and time of the application of the signature and meaning of the signature are displayed and/or printed.	Y	Signatures can be reviewed within the Mastersizer 3000 software system and can be included on result print outs.
§ 11.50 (b)	E-signature information, links to the signed records and the signed information must not be alterable for individuals involved in the business process.	Y	Signatures are directly applied to a record in the Mastersizer 3000 application. If the record is edited or copied, the signature information is immediately removed in the edited / copied version of the record. This prevents the signed record from being changed.
§ 11.70	The system must be designed such that e-signature information including links are saved as read-only data and cannot be excised, copied or transferred to falsify e-records.	Y	The signature is directly applied to the record, and is protected for editing using other windows applications via a hash code. If the record is edited or copied, the signature information is immediately removed in the edited / copied version of the record. This prevents the signed record from being changed.
§ 11.100 (a)	The computerized system must not accept duplicate user accounts.	N	The Mastersizer 3000 software security layer uses the Windows security system to control software access. This requirement will therefore depend on local IT procedures.

21 CFR Part 11 Gap Analysis

21CFR11 Reference	Possible Interpretation	Is this met?	Comment
§ 11.200 (a)	The computerized system must be designed to require two components for the execution of the first e- signature within a session (*e.g. User ID & password*).	Y	The electronic signature feature in the Mastersizer 3000 application requests authentication via the Windows Security system prior to applying a signature. A user's ID and password are both required.
§ 11.200 (a)	The computerized system should be designed to require the private component for the execution of subsequent signings within a session.	Y	Only a user's password is required for subsequent signings of records in the Mastersizer 3000 application.
§ 11.200 (b)	A computerized system using electronic signatures based on biometrics must provide mechanisms that prevent from bypassing the biometric controls.	N/A	Biometrics are not supported within the Mastersizer 3000, accept where the Windows security system has been configured to accept biometric authentication.
§ 11.300 (b)	The computerized system should support password-aging processes (prompts for password r**e**newal after 60 calendar days).	Y	The Mastersizer 3000 software security uses the Windows security system. This should be set up appropriately to meet this requirement.
§ 11.300 (b)	The computerized system should allow for configuration of the password aging parameter.	Y	The Mastersizer 3000 software security uses the Windows security system. This should be set up appropriately to meet this requirement.
§ 11.300 (b)	The setting of the password aging parameter should be limited to duly authorized personnel only.	Y	The Mastersizer 3000 software security uses the Windows security system. This should be set up appropriately to meet this requirement.
§ 11.300 (d)	Check that the system is able to lock a user account after a specified number of failed access attempts.	Y	The Mastersizer 3000 software security uses the Windows security system. This should be set up appropriately to meet this requirement.
§ 11.300 (d)	The computerized system should be able to log unauthorized access attempts.	Y	The Mastersizer 3000 software security uses the Windows security system. This should be set up appropriately to meet this requirement.
§ 11.300 (d)	Preferably the computerized system should be able to detect potential misuse (e.g. log out of users) and notify the responsible individual.	Y	The Mastersizer 3000 software security uses the Windows security system. This should be set up appropriately to meet this requirement.