MadgeTech 4
Secure Software

21 CFR PART 11
Requirement Checklist

21 CFR Part 11 Requirement	Does MadgeTech Secure Software Comply?	No Additional Action Required To Comply?	Comments
The system must be capable of being validated.	✓	✗	The customer must execute the IQ/OQ/PQ to validate that the software is installed correctly and that it operates properly
It must be possible to discern invalid or altered records.	✓	✓	The file format used in the Secure software is proprietary to MadgeTech and cannot be opened in any other piece of software. Only .MTFFS files are able to be saved and/or opened by the MadgeTech Secure.
The system must be capable of producing accurate and complete copies of electronic records on paper.	✓	✓	The MadgeTech Secure software allows the graph and all data records to be printed on paper. In addition, device status, data file statistics, audit trails and other pertinent information may be printed.
The system must be capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA.	✓	✓	All data files may be transferred by e-mail or other means to other users of MadgeTech Secure software, or printed to a secure document in another format such as PDF.
Records must be readily retrievable throughout their retention period.	✓	✓	All data downloaded from a device are automatically saved to an internal secure database, these data cannot be altered, but is always available for the user to generate a visual representation of the data in grid, graph, and statistic format.
System access must be limited to authorized individuals.	✓	✗	The MadgeTech Secure software ensures that only users with a valid User ID and password can gain access to the software. End-user SOPs should be developed and maintained to ensure that users do not share their unique user ID and or password
The system must be capable of producing a secure, computer-generated, time-stamped audit trail that records the date and time of operator entries and actions that create, modify or delete electronic records.	✓	✓	The MadgeTech Secure software maintains an audit trail file on any salient operation performed on the system. The audit trail is secure and encrypted and contains all operations performed by date, time and operator.
Upon making a change to an electronic record, original information is still available.	✓	✓	Changes cannot be made to raw data datasets; however, reports generated by the user may be changed as desired.
Electronic records audit trails are retrievable throughout the record's retention period.	✓	✓	All audit trails are saved as a part of the record and cannot be deleted or modified in any way.

MadgeTech 4
Secure Software

21 CFR Part 11 Requirement	Does MadgeTech Secure Software comply?	No Additional Action Required To Comply?	Comments
The audit trail is available for review and reproduction by the FDA			The MadgeTech Secure software allows the Audit Trail to be printed or transferred electronically for review and reproduction by the FDA.
When any sequence of system steps is important, that sequence must be enforced by the system.			The MadgeTech Secure software does not require any specific sequence of steps or order of operation. The customer is responsible for defining, writing and enforcing any SOPs that require a sequence of steps.
The system should ensure that only authorized individuals can use the it, electronically sign records, access the operation or computer system input or output device, alter a record, or perform other operations.			MadgeTech Secure software requires unique User IDs and passwords to login to the system. Different features are available to different users depending on their level of access. These levels may be defined and created by the user. Defined SOPs should be implemented so the PC requires an authorized login and directs that users cannot share their unique user IDs and or passwords.
The system should be able to check the validity of the source of any data or instructions If it is a requirement of the system that input data or instructions can only come from certain input devices.			MadgeTech Secure software will only accept input and communicate with data loggers specifically designed and manufactured by MadgeTech using MadgeTech's proprietary communication protocol. Each MadgeTech data logger is uniquely identified by an electronic serial number.
(Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals.)			
A documented training, including on the job training for system users, developers, IT support staff should be available.			Users may arrange to purchase on site system training from MadgeTech or provide their own training through testing and the support of MadgeTech's Secure software documentation package.
A written policy that makes individuals fully responsible for actions initiated under their electronic signatures should be in place.			It is the responsibility of the customer to provide a written policy that informs individual users that they are responsible for all actions taken while under their login.
The distribution of, access to, and use of systems operation and maintenance documentation should be controlled.			The customer is responsible for obeying the licensing terms and distribution of the software and documentation that supports MadgeTech Secure software
A formal change control procedure for system documentation that maintains a time sequenced audit trail of changes should be in place.			The MadgeTech Secure software operations document is revision controlled

MadgeTech 4 Secure Software

Signed Electronic Records

21 CFR Part 11 Requirement	Does MadgeTech Secure Software comply?	No Additional Action Required To Comply?	Comments
Signed electronic records should contain the following related information: ▪ Printed name of the signer ▪ Date and time of signing ▪ Meaning of the signing			This name of the signer, the date and time of signing and the meaning of the signing are contained in all electronically signed records and all printed material. The customer is required to define the meaning of signing the document.
The above information should be shown on displayed and printed copies of the electronic record.			All the above information is displayed and printed on all copies of records.
Signatures should be linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification.			Signatures are linked to the original record and cannot be cut, copied, or transferred.

Electronic Signatures (General)

21 CFR Part 11 Requirement	Does MadgeTech Secure Software comply?	No Additional Action Required To Comply?	Comments
Electronic signatures must unique to each authorized individual.			The MadgeTech Secure software will not allow the user to duplicate electronic signatures. MadgeTech recommends that SOPs include a statement clearly defining that only one person is linked to each user ID. The administrator must define the unique user IDs, the user must define their own unique password.
The reuse or reassignment of electronic signatures should be discouraged.			The end user SOPs should state that user IDs are not to be re-used or reassigned to anyone else. User IDs should be inactivated and a new ID created.
The identity of the individual should be verified before an electronic signature is allocated.			The end user SOP should state that the identity of the individual is verified before an ID is assigned. Once a new user is created, an email will be sent to the administrator and user verifying his/her own unique login password. Once verified the MadgeTech Secure software will identify the individual in the future via the user ID and password. The user will be required to enter their username and password.

MadgeTech 4
Secure Software

Electronic Signatures (Non-biometrics)

21 CFR Part 11 Requirement	Does MadgeTech Secure Software comply?	No Additional Action Required To Comply?	Comments
Signatures must be made up of at least two components such as an identification code and password, or an identification card and password.	✓	✓	To electronically sign a record, the username and password need to be entered.
The user's password must be executed at each signing when several signings are made during a continuous session.	✓	✓	MadgeTech's Secure software requires the password to be executed at each signing.
If signings are not done in a continuous session, both components of the electronic signature should be executed with each signing.	✓	✓	To electronically sign a record, the username and password need to entered at each signing.
Non-biometric signatures should only used by their genuine owners.	✓	✗	Users should put in place SOPs requiring that combination of user IDs and password only be made known to the genuine owner.
Attempts to falsify an electronic signature must require the collaboration of at least two individuals.	✓	✗	Users should put in place SOPs that forbid users from disclosing their unique User ID and password.

MadgeTech 4
Secure Software

Controls for Identification Codes & Passwords

21 CFR Part 11 Requirement	Does MadgeTech Secure Software comply?	No Additional Action Required To Comply?	Comments
Controls to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password, are in place.			MadgeTech Secure software will not allow duplicate User IDs.
Procedures must be in place to ensure the validity of identification codes and that they are periodically checked.			The end user's SOP should state that the System Administrator is to periodically maintain active accounts and disable inactive accounts. MadgeTech's Secure software allows the administrator to set accounts to expire automatically.
Passwords should periodically expire and need to be revised.			MadgeTech Secure software allows the administrator to give the user options to make user passwords expire as well as set warnings to notify the user in advance as to when the password is scheduled to be reset. The customer SOP should determine how often and/or when passwords expire.
Procedure for recalling identification codes and passwords if a person leaves or is transferred should be developed.			Passwords cannot be recalled; the administrator can reset the password. The SOP should state that the administrator can only reset a password if the password is lost or stolen, or the user leaves or is transferred.
A procedure for electronically disabling a identification code or password if it potentially compromised or lost should be in place.			The MadgeTech secure software will allow user accounts to be temporarily or permanently disabled. The customer's SOPs will designate an administrator to have this responsibility. Only administrators can change user account settings.
A procedure for detecting attempts at unauthorized use and for informing security should be in place.			The MadgeTech Secure software will detect attempts at unauthorized use. All attempts are recorded and marked clearly in the audit trail. SOPs should be implemented so that a designated user is responsible for reviewing the audit trail for any suspicious activity.
A procedure for reporting repeated or serious attempts at unauthorized use to management should be in place.			The MadgeTech Secure software will detect attempts at unauthorized use. All serious or repeated attempts are emailed to the designated administrator(s). SOPs should be implemented so that a designated user is responsible for reviewing the audit trail for any suspicious activity.

MADGETECH
WE BUILD DATA LOGGERS

MadgeTech, Inc. . 6 Warner Road . Warner, NH 03278
Tel: (603) 456-2011 . Fax: (603) 456-2012 . info@madgetech.com . www.madgetech.com