Measurement Control Corporation
Process Instrumentation, Monitoring and Control
13D Great Meadow Lane, East Hanover, New Jersey 07936, U.S.A.
Web Address: www.mcc-online.com

21 CFR Part 11 Compliance Table for all MCC Products

Paragraph	Product Function	Compliance
Subpart B – Electronic Records		
Sec. 11.10 Controls for closed systems		
11.10	Elaborate security controls and audit trail to ensure the authenticity, integrity and confidentiality of electronic records.	√
11.10(a)	The 21CFR11 compliant products have been developed and validated using FDA guidelines. The software rejects invalid data.	√
11.10(b)	There is a variety of means to generate copies of records in human readable for suitable for inspection, review and copying. The System Administrator should ensure that all system generated data files, reports and plots are read-only. The 21CFR11 compliant products generated audit trail records are read-only.	√
11.10(c)	Records are protected by restricting access to authorized users. The programs use the 21CFR11 compliant access levels to control the flow of information.	√
11.10(d)	The 21CFR11 compliant products provide a multiple level of password control. Individual levels of authorized access include: User, Supervisor, and Maintenance.	√
11.10(e)	A comprehensive audit trail should capture all significant user actions and system conditions, including actions that create, modify or delete data or user ID/passwords. Audit trail records include date, time, user ID, printed name of the user, action, and reason for action. Audit trail files can be copied and printed out.	√
11.10(f)	The System Administrator should make sure that only permitted sequences of steps are allowed.	√
11.10(g)	All functions should check access authority.	√
11.10(h)	The source of data should be verified through electronic means.	√
11.10(i)	SOP	N/A
11.10(j)	SOP	N/A

11.10(k)	SOP	N/A
11.30	This version of the 21CFR11 compliant products is designed for closed systems.	N/A
11.50	Use the electronic signatures of electronic records for this version of the 21CFR11 compliant products is optional.	N/A
11.70	Use the electronic signatures of electronic records for this version of the 21CFR11 compliant products is optional.	N/A
Subpart C – Electronic Signatures		
11.100	Use the electronic signatures of electronic records for this version of the 21CFR11 compliant products is optional.	N/A
11.200	Use the electronic signatures of electronic records for this version of the 21CFR11 compliant products is optional.	N/A
11.300 – Controls for identification codes/passwords		
11.300	The 21CFR11 compliant products provide a multiple level of password control. Individual levels of authorized access include: User, Supervisor, and Maintenance.	√
11.300(a)	System requires that each User ID and password combination is unique.	√
11.300(b)	Password aging feature is enabled. If password has expired, a user with proper authority is required to enter a new password for a unique user name – password combination.	√
11.300(c)	Supervisor and Maintenance level access has authority to disable user accounts and to reset passwords.	√
11.300(d)	3 or more invalid login attempts are recorded in audit trail.	√
11.300(e)	SOP	N/A

Features:

- Password protection
  - The levels of authorized access include: User, Supervisor, and Maintenance.
    - Operator can do any routine task of the host program.
    - Supervisor can everything Operator can do plus add/edit/delete User Names / Passwords and display Audit Trail (current & historical).
    - Maintenance User can: change system settings, such as calibration, etc.
  - All major activities are governed by access level control.
  - User name is case insensitive, password is case sensitive.
  - Passwords are required to have at least 6 characters, including 1 numeric and 1 alpha.
  - Logout results in an immediate Login screen.

- Password aging feature. The length of aging period is under the System Administrator's control.
- Proper login or program termination is required after a period of inactivity. The length of such period is under the System Administrator's control.
- Failed password logons trigger audit trail.
- User names and passwords are stored in a MS Access Database that is itself protected by the Master Password.
- Assured uniqueness of every user name – password combination.
- User friendly password control that allows multiple sessions of add / edit / delete.
- Authorization (special login) required for password control (Authorizing User is not necessarily the Current User).
- Master Password for system administration and maintenance.

➢ Audit Trail
- Audit Trail is designed to record important actions, including modification of files and folders. All major actions are governed by audit trail control.
- New Audit Trail file is created each time the program is run. The System Administrator can specify the folder for Audit Trail files.
- Audit Trail files are tagged / named with the use of Date and Time of creation.
- Audit Trail file maintenance (backup, deletion) should be governed by procedural control (SOP).
- Some user actions may require a reason entry. The program does not proceed until the reason for change is given,

➢ General
- All vital data and reports have read-only attributes.
- Touch Screen functionality is optionally enabled.
- All MCC products are closed (stand-alone) systems.
- Use of electronic signatures with MCC products is optional.