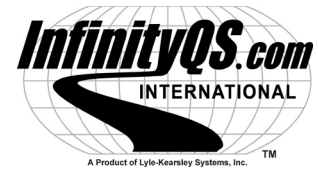


Understanding:

# SPC & 21 CFR Part 11

## Part 1: Access Control



Douglas C. Fair  
Co-Director of Statistical Applications  
InfinityQS International, Inc.

### Statistical Process Control & 21 CFR Part 11: Access Control

By now, we should all understand the value that Statistical Process Control (SPC) can provide an organization. By improving the quality, consistency and acceptability of manufactured articles and reducing scrap and rework, companies have saved millions of dollars with their SPC investment. Now that the FDA's 21 CFR Part 11 is a reality, many companies are trying to understand what must be done to insure their SPC investment complies with these regulations.

There are several key areas that must be considered when choosing and deploying an SPC system to comply with the FDA's requirements. These include hardware, software and procedural requirements. To cover the entire scope of these requirements could easily consume the contents of this magazine. Therefore, we will limit this article to one specific area... *Access Control*.

### Controlling System Access and Control

Knowing who is accessing your SPC system and controlling their actions might seem simple enough. Just ask for their name as they enter the application and make sure to associate that name to any action performed. Fundamentally that's right. But, according to 21 CFR Part 11 that's not enough, and for good reason. Let's look at what must be done to comply with Part 11.

- 1. Users must be uniquely identified.** To gain access to the system the user must first enter a login name and a separate password that uniquely identifies the user. No other user can have the same combination of login name and password.
- 2. Passwords must be encrypted.** Passwords stored in a database must not be readable by anyone accessing the database. Therefore, it is imperative that all passwords are encrypted before they are written to the database.
- 3. Passwords must be secret.** Not even a security administrator should know another user's password. After a security administrator assigns a user password, the user must immediately change it.

A screenshot of a software configuration window titled "Electronic Signature Requirements (21 CFR Part 11)". The window contains several sections with checkboxes and input fields:

- Password Configuration:** Includes checkboxes for "Encrypt Passwords" (checked), "Minimum Password Length" (8 Characters), "Minimum Password Age" (Days), and "Maximum Password Age" (30 Days).
- Password Recycling:** Includes a checkbox for "Prohibit Recycling of Passwords for:" (180 Days).
- Stale Accounts:** Includes a checkbox for "Revoke User Account if Idle for:" (30 Days).
- Account Lockout:** Includes checkboxes for "Number of Bad Logon Attempts:" (3 Attempts) and "Reset Count after:" (30 Minutes). It also has radio buttons for "Lockout User's Account Forever" (selected) and "Lockout Duration:" (Minutes).
- Access Logs:** Includes checkboxes for "Create Log of User Access" and "Create Log of Access Violations".

Buttons for "OK", "Cancel", and "Help" are visible on the right side.

- 4. Passwords must have a minimum length.** A minimum password length must be enforced by the SPC system. Too short a password makes it easy to decipher while a long password is more difficult to remember. A good minimum password length is between six and eight characters.

5. **Passwords must be changed if their security is compromised.** If a user believes that their password has become known, the user should immediately change it.
6. **Passwords must be changed periodically.** The system must specify a maximum password age. Once the password has expired the user must change their password before access to the system is granted. Maximum password age should not extend beyond 90 days and more appropriately be set to 30 days.
7. **Password recycling must be prevented.** Users must be prohibited from switching between two or three "favorite" passwords during password changes. A good practice would be to inhibit the reuse of previously used passwords for six to twelve months.
8. **Stale accounts should be closed.** If a user's account remains inactive for a period of time the account should be prevented from further use.
9. **Limit attempts to access system.** After several unsuccessful attempts to gain access to the system, the user's account should be locked and their password revoked. This action is taken to prevent someone from breaching the security barrier of the system. When an account is locked out, an administrator should be required to re-set the user's password in order to reinstate system access. The number of access attempts should be limited to three or less.
10. **Maintain a log of all security violations.** The system must create and maintain a log of security violations by individual users. Violation examples include failing the consecutive sign-in rule as specified above and attempts to edit or delete data when not authorized to do so. The log should at a minimum contain the user, the violation, and the time and date.
11. **Limit access based on needs.** Security privileges should be appropriate to the individual's function. For example, a shop floor operator should be able to enter data but not create control limits. Likewise, a quality manager should be able to create control limits, but not create specification limits.

## **Conclusion**

At first glance, the FDA's 21 CFR Part 11 appears to be a set of imposing requirements to manufacturers trying to implement their quality system. Yet, it is based on sound principles of security and traceability that must be part of all quality systems. Broken down in logical steps, the inclusion of these requirements becomes a straightforward and systematic task of following the rules.

## **About the Author**

Douglas C. Fair is Co-Director of Statistical Applications at InfinityQS International, and is the co-author of two books on statistical applications: *Innovative Control Charting, Practical SPC Solutions for Today's Manufacturing Environment* (ASQ Quality Press, 1998) and *Principles and Methods for Quality Management in Health Care* (Aspen Publishing, 2000). Fair holds a Bachelor of Science degree in Industrial Statistics from the University of Tennessee in Knoxville and is a member of the American Society for Quality. Mr. Fair can be reached by email at [dfair@infinityqs.com](mailto:dfair@infinityqs.com).

For further information contact [sales@infinityqs.com](mailto:sales@infinityqs.com)

Telephone: 1.703.393.2222

Toll Free: 1.800.772.7978

Facsimile: 1.703.393.2211

Copyright © 1999-2000 Lyle-Kearsley Systems, Inc.  
All Rights Reserved.