

Conformance of *SQCpack* to Code of Federal Regulations, 21 CFR 11.1

If an organization has determined that 21 CFR 11.1 is applicable to the maintenance quality data/chart records, PQ Systems, Inc., recommends that users of *SQCpack* implement the following steps to ensure compliance. In order to be compliant with 21 CFR 11.1, the *SQCpack* user needs to do the following:

1. Require User Login with password when *SQCpack* is accessed.
2. Limit user access to *SQCpack* databases using user rights supplied with your Operating System.
3. Set the computer to time-out after a specified time interval when no action has occurred. A password should be required in order to get back in. Setting passwords is also a function of the Operating System.
4. Enable Auditing. Additional security provisions that are offered by the *SQCpack* software to meet the requirements of the Code include the following:

A. **Electronic signature:** *SQCpack* may be set to require an individual login with a unique, current password (using User Login required). Only a user with appropriate rights can create users or make them inactive. Using User Login, a login name cannot be re-used. The admin user can globally designate the period of time for which a particular password can be used without expiring.

B. **Auditing:** In the current version of the software, an auditing feature can be activated to record the identities of all who sign in, as well as all their activities after sign-in. Each activity records date and time, event type, user name, reason, and specific details of any information that was changed. These fields are automatically filled with the identity of the individual signed in. The Reason field can be set to be required for various actions such as when records are modified or deleted.

C. **Access:** A user's access rights can be limited by means of the User Access Form, completed at the time the user's identity is created. (A user's access rights can be modified at a later date by an individual with appropriate rights.) In general, users may be restricted from or given permission to add, edit, or delete data groups, data, charts, choice lists, list filters, etc. Permission to access other activities can be restricted. Access rights can be limited to as little as View only.

D. **Data entry:** Using choice list options, data entry can be set so the user can be required to match an item on the corresponding choice list.

