

## Conformance of *GAGEpack 9.0* to Code of Federal Regulations, 21 CFR 11.1

If an organization has determined that 21 CFR 11.1 is applicable to the maintenance of its gage records, PQ Systems, Inc., recommends that users of *GAGEpack 9.0* implement the following steps to ensure compliance.

In order to be compliant with **21 CFR 11.1**, the *GAGEpack* user needs to do the following:

1. Use *GAGEpack 9.0* and enable security by using Full Login required.
2. Limit user access to *GAGEpack* 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 the Audit trail.
5. On the toolbar for Inventory tab, the user can add a lockout icon. This will permit the user when leaving *GAGEpack* open to require the user's password to be entered before *GAGEpack* can be used again.

Additional security provisions that are offered by the *GAGEpack* software to meet the requirements of the Code include the following:

1. **Electronic signature:** *GAGEpack 9.0* may be set to require an individual login with a unique, current password (using Full Login required). Only a supervisor can create and delete users, although this right can be extended to other designees. Using Full Login, a login name cannot be re-used, even after a user name has been deleted and is no longer allowed to sign in. The supervisor can globally designate the period of time for which a particular password can be used without changing it.
2. **Audit trail:** In the current version of the software, an audit trail feature can be activated to record the identities of all who sign in, as well as all their activities after sign-in. Each event has an "entered by" or "done by" and sometimes both. These fields are automatically filled with the identity of the individual signed in. Each field can be required to have an entry (cannot be left blank). (See validation criteria below.)
3. **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 given permission to add, edit, or delete events and activities. Permission to access other activities can be restricted. Access rights can be limited to as little as View and Print Reports.
4. **Events:** Using validation criteria, many of the fields in *GAGEpack 9.0* can be set to require an entry to be made, and, in some cases, the user can be required to match an item on the corresponding choice list.

