

# General Guidelines for Implementing Information System Controls

Each county official is responsible for implementing controls over the office's computer operations. These include general controls that relate to the overall environment and application controls that relate to the transactions processed in the accounting software. The following is an overview of suggested controls that should be in place in each county office that utilizes a computer system to maintain financial information. This list may not be all inclusive. The official should review all procedures in the office to determine proper controls are in place. **Officials should keep in mind that they are responsible for establishing and maintaining a system of internal controls for their office.** The Division of County Audit cannot make management decisions on your behalf neither can our audit be considered an internal control procedure.

## General Controls

- All offices should have a policies and procedures manual for computer operations. This manual should provide an adequate basis for the managing, planning, controlling, and evaluating the office's computer resources. The manual should address the following items:
  - System startup and shutdown
  - System access and security
  - Backup procedures
  - Hardware/software maintenance
  - Budgeting of computer equipment
  - Hardware disposition
  - Virus prevention
  - Output distribution
  - Day, month, and year-end routines
- All offices should have a disaster recovery plan. The plan should describe the actions to be taken in the event of a disaster that disables the computer system. The plan should include the following items:
  - Emergency and employee telephone numbers
  - Disaster recovery checklist
  - Off-site storage location of backups
  - Manual processing procedures
  - Priority listing for the applications
  - Contingency operations site
  - Current computer inventory listing
  - Comfort letter from the vendor noting planned response to a disaster

A copy of the plan should be maintained in the office as well as at an off-site location.

- Backups should be performed on a daily basis. There should be a backup labeled for each day of the week and these backups should be stored in a secure location within the office. Two sets of weekly backups should be maintained and rotated to an off-site storage location on a weekly basis. An appropriate off-site location would be another county office building or a lock box at a bank. Year-end backups should also be performed and stored off site. A backup log should be maintained. Each time a backup is performed, an entry should be made to the backup log. This log should include the initials of the person performing the backup, date of the backup, type of backup (daily, weekly, etc.), and the specific storage location of that backup. At least once a year, backups should be tested to ensure reliability. This verifies that the backup media (disk, tape, etc.) being used is in good condition and that the backup software is operating properly. It should be noted that vendors may also provide remote backup services to the county.
- Security should be used at the operating system level. In order to access the operating system, users should be required to enter a unique login and password. This password should be changed at least once every 90 days. Also, the screen saver should be enabled and password-protected and any guest accounts should be disabled or renamed. Passwords should not be written down or shared by employees.
- All users of the system should sign an acceptable policies and use agreement form. This form should state the acceptable use policies of the office regarding Internet and email activities. Most importantly, it should state that the users do not have any expectation of privacy when using the county's information system resources and that users are responsible for all transactions performed using their individual passwords. It should be emphasized that passwords should not be shared or disclosed to others.
- Operating system updates should be installed on a regular basis.
- Virus detection software should be installed on all computers. Virus definitions should be regularly updated.
- Only authorized personnel should have keys to the office.
- All negotiable documents should be stored in a secured location when not in use.

## **Application Controls**

- To access the accounting software, users should be required to enter a unique username and password. A unique username and password should be assigned to each employee and these passwords should remain confidential. These passwords should be changed every 90 days. If an employee leaves employment, his/her login should be removed from the system immediately.
- The software should not allow users to alter or delete receipt or disbursement transactions without leaving an audit trail.

- The software should not allow users to alter or delete customer accounts without leaving an audit trail.
- The software should not allow users to alter or delete general ledger entries without leaving an audit trail.
- If the accounting software captures alterations or deletions in an audit log, this log should be reviewed by management on a regular basis.

**If you should have any questions regarding IS controls, please contact:**

Penny Austin  
Division of County Audit  
[penny.austin@tn.gov](mailto:penny.austin@tn.gov)  
615-401-7841