

## SECTION C-15

### DESKTOP COMPUTING MANUAL

#### Sections

- [1.00 Policy Acceptance](#)
- [2.00 Equipment Registration and Assignment](#)
- [3.00 General Microcomputer Use](#)
- [4.00 Security](#)
- [5.00 Backup and Storage](#)
- [6.00 Microcomputer Training](#)

#### 1.00 POLICY ACCEPTANCE

##### 1.10 Policy Acceptance

All employees are expected to be aware of, and abide by, the requirements of the General Computing Guidelines.

#### 2.00 REGISTRATION AND ASSIGNMENT OF HARDWARE/SOFTWARE

##### 2.10 Equipment Registration

All computer hardware and software purchased by Internal Auditing will be logged by the Assistant to the Director. This inventory listing will include registration or serial number, description and date the item was purchased.

##### 2.15 Warranty Registration

All computer hardware and software purchased by Internal Auditing will be registered with the manufacturer (or in accordance with the product's registration policy). The Assistant to the Director will complete the registration. A copy of the registration form and/or license agreement will be maintained by the Assistant to the Director.

## 2.20 Assignment of Hardware/Software

Microcomputer equipment and software will be assigned by the Director of Internal Auditing.

## 2.30 PC Configuration Notebook/File

The Assistant to the Director and the Assistant Director will maintain a notebook and file which lists the current hardware and software owned by the Internal Auditing Department, and its location. This file will also include about a description of the standard desktop configuration, including required utility programs.

## 3.00 GENERAL MICROCOMPUTER USE

### 3.10 System set-up

All desktop/laptop systems within Internal Audit will be set-up and configured in essentially the same way (standard application software, standard operating systems and system files, common main menu, etc.). This configuration has been developed by the Assistant Director. Audit staff assigned to maintain standard desktops and perform regular updates and maintenance will meet with all staff monthly. Revisions to menus, operating systems or files will be made only under the direct supervision of the audit staff assigned to the task. Suggestions for changes to standard set-ups or required changes should be referred to these individuals.

### 3.20 Assistance/Problems

Problems with hardware or software should be reported to the Executive Support Staff via email, or the desktop link to the Executive Support Help Center. If you do not have a desktop link to the Executive Support Help Center, please notify the Assistant to the Director so that she can arrange for it to be installed. If you require immediate assistance, the Executive Support Staff can be reached using the phone numbers listed on the Help Center's home page.

### 3.30 Environmental Control

Hardware and software should not be exposed to extreme heat or cold. Avoid leaving equipment in any abnormal environment. Consideration should be given to moisture and humidity when storing equipment or media. All hardware should be safeguarded from electrical surges through the use of surge protectors. Potentially harmful activities, such as eating, drinking or smoking near microcomputers are strongly discouraged. Magnets can be totally destructive to magnetic storage media and many desk accessories now include magnets. Extreme care should be

exercised when diskettes are used near magnets. Magnets should also be kept away from CPU units and monitors.

#### 3.40 Equipment Transportation

Care should be taken during the transportation of hardware and software. Coordinate movement of non-portable equipment with the Assistant Director and Assistant to the Director to maintain inventory records and physical safety.

#### 3.50 Recovery of Lost Data

In case of data loss, contact the Assistant Director or the IT Support Staff Assigned to the Audit Department. The IT Support Staff can be reached through the "Exec Support Help Center" icon on the desktop, or by contacting the Assistant to the Director.

#### 3.60 Documentation and Manuals

The user manuals library will be maintained in the offices of the Assistant to the Director and Assistant Director. Extra copies of the manuals may be checked out of the Departmental Library.

#### 3.70 Use of Licensed Software

It is the policy of Internal Auditing to comply with all contractual obligations contained in the license agreements to which it is a party. Consequently:

- All purchased software must be registered, as applicable, with the vendor. All audit staff will register products as they are received.
- Licensed software and accompanying documentation is prohibited from being duplicated, modified, sold, traded or otherwise disseminated by any employee if contrary to the vendor's license agreement.
- Copies of software shall not be purchased or otherwise accepted by any employee from any source if it is known, or should have reasonably been known, that such copies were made contrary to a vendor's license agreement.
- You have the responsibility to take reasonable actions to secure all copies of licensed software when not in use.

You are responsible for the software on your computer and should ensure adherence to the terms and provisions of all relevant license agreements.

Software issued to Internal Auditing should not be used on computer equipment other than that assigned to Internal Auditing, unless specifically authorized and approved by the Director of Internal Auditing or his designee.

### 3.80 Password Protection

Departmental passwords should use the following standards:

- A minimum of five to eight characters, preferably a combination of letters and numbers;
- Not obvious/easily guessed (nicknames, date of birth, etc.), Changed on a regular basis,
- Not shared with other users; and
- Not written down and easily accessible/visible to other persons.

## 4.00 SECURITY

### 4.10 Physical Security

Computer hardware and software must be protected from unauthorized use, vandalism, theft and inadvertent damage. Employees must see that due care is exercised in safeguarding microcomputer equipment and software. Proper precautions must be taken to ensure that the equipment is well protected.

- Computer equipment should be stored in a secure environment. The security of the environment should be assessed and reasonable measures taken to adequately protect the equipment. For example, locking portable computers in file cabinets or covering equipment when overhead maintenance is being performed.
- All laptop computers will have a cable-lock for use in the field. In addition, laptop computers should be locked in a desk drawer when leaving for the day. .
- Use good judgment (or ask EDP audit staff) when leaving hardware and/or software unattended for a long period of time.
- When appropriate, use password protection provided in the software (WordPerfect, Norton Utilities, etc.), hardware or physical locking devices to protect sensitive data.
- Output should be controlled according to its nature. Material of a sensitive or confidential nature should be handled and stored to ensure access only by appropriate personnel.

### 4.20 Security from Viruses and Spyware

The possibility of computer viruses and spyware being introduced into Internal Auditing's systems can be greatly reduced through the following practices:

- Files from any outside source should be scanned with virus detection software before loading software or opening files.
- Any software retrieved from external networks (bulletin boards, free/share ware) must be approved in advance by the Assistant Director.
- Virus Scan software should be set to perform automatic updates and run at least weekly.
- Spyware removal software should be updated and run at least once per week.
- Keep archived backups of your data files. This is the best defense against total loss of data in case of virus or hardware failure.

#### 4.30 Data

Data integrity and confidentiality must be maintained. Application software should be locked in the file room when it is not in use.

- 1.) Removable storage media should be properly labeled and stored in their protective container when not in use.
- 2.) Never attempt to reformat the hard disk.
- 3.) Use good judgment (or ask for advice) when maintaining and storing removable media.

### 5.00 BACKUP AND STORAGE

#### 5.10 Need for Backup

Information on the "I:" drive is backed up regularly during the day. However, data in the computer's memory is not saved until it is "written" to hard disk or removable storage media. Employees must periodically save data and use proper backup procedures. Proper backup procedures include creating and maintaining additional copies of pertinent information maintained on personal computers. It is the responsibility of the user to create backup copies of their data files. A power failure, hardware failure, diskette problem, virus or even accidental key stroke can cause a partial or complete loss of data.

#### 5.20 Hard Disk Files

Hard disks increase the efficiency and speed of data storage and retrieval; however, a hard disk failure may cause a significant loss of data. All data files maintained on the hard disk should be periodically backed-up. CD's will normally be used for hard disk backup. Backup copies should be properly labeled and secured.

#### 5.30 Storage of Audit Work Papers on Removable Storage Media

Back-up copies of all audit working papers are stored on CD as well as in paper format. Work paper documentation received via e-mailed files should be included in the working paper files to

help ensure that it is retained with the other working papers. Documentation received on CDs or other removable media should be included with the paper file. The location of these CDs should be listed in the audit workpaper file and the CDs should be adequately labeled and stored.

#### 5.40 Software Documentation

Documentation should include, for each program:

- Program name
- Category (Payroll, Accounts Payable, Personnel, etc.,)
- Purpose (brief description of what the program does)
- Date(s) (developed, revised)
- Comments (additional brief information)
- Source code
- Date and name of preparer

In addition, at least one other person should be trained in the use of programs deemed critical to the Department.

### 6.00 MICROCOMPUTER TRAINING

#### 6.10 Training

Training is available through numerous sources both on and off campus. Training needs will be continually assessed by the management of Internal Auditing to update the required training schedules. If you have interest in a particular training program, please bring it to the attention of the Assistant Director.