INSTITUTIONAL DIRECTIVE 2-3

November 27, 2006

Title: Information Services

I. Purpose

This directive sets forth the policies and procedures necessary for the proper operation of Piedmont Technical College's Information Services Department.

II. Policy

It is the policy of Piedmont Technical College to establish a centralized institutional computer system and to install and support desktop Personal Computers for all faculty and staff in order for them to provide current and reliable data in support of the administrative decision-making within the college.

III. Philosophy

The function of the Information Services Department of Piedmont Technical College is to provide and maintain computerized systems for the institution. Its purpose is to insure the quality, availability and utility of the information necessary for the Institutional Officers and members of the staff to properly administer the affairs of the college and perform the routine tasks of each functional area of the college. Included in these systems are a centralized database system, a network infrastructure and desktop client systems.

IV. Use of Computer Equipment

A. College faculty and staff will be provided the use of a modern personal computer running the most currently approved operating system and application software. The supervisor or department head of a new employee will request computer access by calling IS Customer Support or going to the Online Employee Center on the College's WebPage to submit the Account Request Form. Training of new faculty and staff is the responsibility of the person's supervisor or department head. Information Services will be available to assist in training upon request.

B. Information Services, via the use of a IS Customer Support system will maintain, repair and update the desktop platforms. Upon discovering a problem with the desktop PC or installed software, administrative users should contact IS Customer Support at the published phone number or email address.

C. Upon being notified of problems, IS Customer Support personnel will record the incident and dispatch a technician to resolve any issues.

D. Technicians will enter an administrative office only under escort provided by the responsible office.

Office of Responsibility: Senior Vice President

V. Computer Systems Maintenance

The Director of IS at Piedmont Technical College has the administrative responsibility for overseeing the maintenance of the college's computer systems. This responsibility includes that of ensuring that all operational policies and procedures necessary for the successful use of those systems are periodically reviewed and where necessary, revised. It is also this individual's responsibility to supervise all aspects of the procurement, installation and maintenance of all computer equipment used as part of the system. All purchases of administrative Information Technology equipment and software will be reviewed by the Director of Information Services for compliance with existing standards.

VI. Security

A. Facility - The Computer Center is a controlled access room. This is necessary as much of the administrative data processed by the Computer Center pertains to the academic records of students, personnel records of the staff or financial affairs of the college. Only persons authorized by the College are to have keys to the Center.

B. Programs - The access to programs making up the college's Information Systems will be controlled by the Director of IS and his/her staff. No individual in a functional area of the college should grant program or data access to another person without determining if that individual is authorized

C. Reports - All reports generated by the college's IS system will be handled at all times in a responsible manner. The same degree of confidentiality and discretion that staff members exercise in the daily handling of information in the performance of their normal job-related functions will also be followed in the dealing with information and reports generated by the institution's computer system. Such information and reports will be treated as confidential at all times and will ~~should~~ not be shown or discussed in an indiscriminate manner. Reports ready to be discarded that contain confidential matter will be shredded

D. Passwords - Each IS customer accessing the college's computer system will be given passwords at the time access to the systems is granted. Some passwords automatically expire periodically and a new password must be assigned. Only the person specified to log in to a given account/username may know that password. When a customer forgets a password, the IS staff will assign a new one. Passwords should be a least 6 characters and/or numbers in length and should not be words listed in dictionaries, personal names or words that can be easily guessed. If a customer determines that someone has learned his/her password, it is to be changed immediately.

E. In the event of a situation where the customer determines that the above rules for establishing and maintaining passwords should be suspended or changed for an account, the customer will provide a request for variation to the Information Services Director. If the director determines that the request is justified, he/she will issue and retain a Variation to Security Policy stating the circumstances of the divergence from policy.

VII Disaster Recovery

A. In the event of a loss of data files, the Director of IS is responsible for recovering the lost data. In order for recovery to be possible, the data must have been copied and stored in a safe place and be accessible at all hours to IS personnel. If for some reason, all or a portion of the computer center hardware is damaged beyond repair, or a situation occurs where the system will be out of order for a period of more than forty-eight hours, it is the responsibility of the Director of IS to provide alternate means of continuing with normal business until the hardware can be replaced.
   1. All data stored on the college's Servers will be backed up on a regular schedule and the backup media will be stored in an appropriate location.
   2. Backup files will allow the data to be restored to its original state based upon the backup schedule of the affected server.
   3. Backup files will be transported to the storage location within twelve hours of the completion of the backup.
   4. Backup media will be retained for at least three weeks. If backups of historical data are to be maintained for a longer period, the office requiring the longer retention schedule will provide storage requirements in writing to the Director of IS.

B. A Disaster Recovery Plan will be held on file in the college and at a remote site. The Disaster Recovery Plan will delineate the steps needed to restore the system on alternate equipment until the computer center is restored to normal use and should be usable by contract personnel if computer center personnel are not available for the recovery. The Disaster Recovery Plan will be tested each year to determine if the plan and the alternate site are satisfactory. The plan will be implemented when the president or his designated representative declares the situation to be a disaster.
   1. The Director of IS will make necessary arrangements for an alternate site to be designated as the Disaster Recovery Hot Site. The Hot Site will be one of the county centers. The Hot Site will have sufficient hardware, software, network connections and backups to continue normal operations once the site is occupied and brought on-line.
   2. Upon declaration of a disaster, all available computer center personnel will report to the hot site and begin restoring the system.

Original on File **11/27/06**

Approved for Publication **Date**