TITLE:	**Information Technology**
PROCEDURE NUMBER:	**4-4-1060.1**
RELATED POLICY AND PROCEDURES:	**4-4-1060 Information Technology**
DIVISION OF RESPONSIBILITY:	**Business and Finance**
PAGE:	**1 of 3**

July 11, 2013	**November 15, 2022**	**October 30, 2019**
Approved by President	**Date of Last Review**	**Date of Last Revision**

Administrative Responsibilities

It is the responsibility of the Information Technology (IT) Department personnel to review and revise this procedure to assure proper operation of the computer systems for the College.

Procedure

Piedmont Technical College (PTC) provides a centralized technical support infrastructure to meet the computer and network communication needs of the college administration, faculty, staff, and students through the process of strategic planning, resource management, and customer service. Included in the oversight is the management of multiple centralized database systems, network infrastructure, unified wireless communications and data service, web-based forms, unified helpdesk services, student laboratory and classroom management, technology training, integrated maintenance of safety and security systems, and other technologies to support its employees and students.

1. PTC provides College employees with the use of personal computers, operating systems and application software. Once entered into the College's Enterprise Resource Planning System (ERP) (Banner) new employees receive a network account. It is the responsibility of the Supervisor of the new employee to request through the help desk

ticket system the needed levels of security. Training of new faculty or staff is the responsibility of the employee's Supervisor.

2. The technical support help desk maintains, repairs, and updates desktop platforms. Upon discovering a problem with your administrative pc, lab or smart classroom, users shall contact the help desk at the published telephone extension or submit a help desk ticket via the PTC website. Submitting a help desk ticket should ensure a faster response time to any issues you may be experiencing.

   a. Upon notification of the problem, the helpdesk manager, if unable to resolve the issue, will assign the ticket to a technician who will assist with resolution.

   b. Technicians have access to all offices, with the exception of the Colleges' administrative office areas. Technicians enter administrative offices only when escorted by the responsible office designee.

B. Computer Systems Maintenance

1. The Chief Information Officer has the administrative responsibility for overseeing maintenance of the College's computer systems. This responsibility includes conducting periodical reviews and when necessary, revision of all operational policies and procedures necessary for the successful use of the systems.
2. The Chief Information Officer maintains and publicizes a schedule of routine maintenance requiring down time. It is also this individual's responsibility, and that of any team leaders, to supervise all aspects of the procurement, installation and maintenance of all computer equipment used as part of the system. All individuals requesting the purchase Information Technology equipment and software must review the request with the Information Technology Department to ensure the technology requested complies with existing standards. The Information Technology Department may be unable to provide technical support for any purchases not in compliance with the College's IT standards.

C. Security

1. Facility:

   The server room is a controlled access room. To protect student academic records, personnel records and the financial affairs of the College, only persons authorized by the College are to have access to this room. This access also applies to network closets and network switch areas. A fire suppression system protects the server room and Hot Site. Individuals must take precautions to disable the fire suppression system when working in the server room. To gain access to the server room to complete work orders, individuals must contact Campus Police and Security.

2. Reports:

   All reports generated by the College's IT department are at all times responsibly handled with confidentiality and discretion, especially when handling sensitive

information generated by the institution's computer systems. The College prohibits the indiscriminate sharing or discussion of these reports. When discarding reports containing confidential information, shredding occurs.

3. Passwords:

   Each user enters a password to access the College's network computer system. On the first login, the user is required to reset their password. All passwords automatically expire. Only the person specified to log in to a given account/username may know that password. When a user forgets a password, security questions allow the user to reset the password. If needed the user can contact the PTC helpdesk for assistance. IT will never request your password via email. A compromised account may be temporarily disabled. A user should be immediately notify IT once aware that their account is in a compromised state.

D. Disaster Recovery

1. In the event of a loss of data files, the Chief Information Officer is responsible for recovering the lost data. In order for the recovery to be possible, the data must have been stored in a safe place accessible at all hours to IT personnel. It is the responsibility of the Chief Information Officer to provide options for alternate means of continuing normal business until the replacement of hardware occurs.

   a. The archiving of all production critical data to the Hot Site on the College's servers occurs periodically.

   b. Operating systems for servers are periodically stored.

   c. The maintenance of other equipment backups appears at a period that allows for minimum down time.

2. The Chief Information Officer makes necessary arrangements so that sufficient storage is available at Hot Site.

3. Upon declaration of a disaster, all available computer personnel shall report to the Hot Site and begin restoration of the system.