2.14 COMPUTER INFORMATION SYSTEMS

Last Revised: January 2011

Policy Statement: Information systems are a valuable asset, critical to the success of Piedmont Community College and its mission. These systems include network and server systems on which the college depends. The College accepts its responsibility for managing and protecting the accuracy, security, and availability of these sensitive resources to meet the needs of the college and its mission. This policy provides governance to meet the requirements of legitimate access to information systems.

Purpose/Definitions: N/A

Approval Authority/Monitoring Authority:
The management of Piedmont Community College’s computer and technology resources is exercised by the data custodian and data owners through the office of management information systems. This management will focus on protecting the accuracy, security, and availability of information resources.

Procedure:
Data Custodian: The President, as CEO of Piedmont Community College, shall be the data custodian of all data and other information assets of the College. The data custodian has the ultimate responsibility for the protection of these resources and has the responsibility for approving procedures designed to meet these requirements.

Data Owners: The Vice Presidents, as heads of the operational areas of the College, will serve as the data owners for their respective areas. The data owners will assist the data custodian in the management and control of information assets. When appropriate, the data owners may appoint, in writing, an alternate to assist when they are unavailable to support this activity. The data owners will be responsible for reviewing and approving in writing any changes in security settings, access rights, or other configurations. Data owners will review security access for individuals who have access to their area of ownership.

Management Information Services (MIS): MIS shall implement all authorized changes requested and approved by the data custodian or data owners. If MIS feels that the authorized changes are in conflict with best practices, MIS will recommend solutions or alternatives to the appropriate data owner or data custodian.

MIS will not change security settings, access rights, or other configurations without first receiving proper authorization from the data custodian or owner. In an emergency situation when immediate action is required, MIS may make changes without the proper authorization but is required to document the event and report the facts to the data custodian or owner for concurrence of the actions taken.

MIS will recommend and develop local policies and procedures addressing significant issues of the day-to-day operation of the information systems under its control.

MIS will maintain copies of all approvals issued by the data custodian and data owners.

Notification: In most instances, e-mail authorizations from the appropriate data owner will be acceptable in lieu of written documentation.

Legal Citation: N/A
History: Effective July 1991, revised January 2008, reviewed May 2010