ADMINISTRATIVE PROCEDURE No. 8300

Administrative Data

Date Adopted: 21 May 2002

Date Revised: 11 December 2009

Date Reviewed: 28 May 2014

References: Student Code of Conduct Policy

A. Access to Administrative Data

Administrators, faculty, and staff are to access only those data and transactions that are required in order to conduct their officially assigned duties. Information can only be released according to the guidelines within each unit and in accordance with existing College policies on the release of information.

Controls over information systems should provide the ability to trace violations of security to individuals who may be held responsible.

Employees who attempt unauthorized access to administrative computers are subject to disciplinary measures as per College policies.

Supervisors have the following responsibilities:

1. Periodic review of access granted to their staff
2. Upon the conclusion of the work day that staff have properly secured administrative information
3. Developing and implementing procedures for maintaining access security, including education of their constituency on these procedures

B. Responsibilities of Authorized Users

Any person authorized access to any information:

1. is not to make or permit unauthorized use of any information.
2. should ensure the identity of the information recipient before discussing information pertinent to the individual's record.
3. may not use non-public institutional information for personal or financial gain, or malicious purposes
4. may not obstruct its use for legitimate institutional need.

C. Handling of Confidential Information
The improper access to or unauthorized disclosure of confidential information is a violation of College policies may be a violation of state, federal, or U.S. laws that pertain to the College.

Computer screens must be oriented to prevent unauthorized people from reading sensitive information.

Printed output containing confidential or sensitive information must be treated with the same care as confidential data files.

Floppy disks, cartridges, and external storage drives, and removable media with sensitive or confidential information must be stored in a secure area or in a locked file cabinet or desk.

Storage of non-electronic forms of administrative information must safeguard against the information's unauthorized viewing as well as loss due to accidents or acts of nature.

D. Disposal of Confidential Information
Paper and microfiche copies of sensitive and confidential information must be disposed of either by burning or by shredding to ensure the security of the information.

Properly discard computer disks (hard disks and floppy) containing administrative, confidential, or sensitive information. Procedures for properly erasing computer disks can be obtained from the College Information Technology Office.

E. Data Integrity
Data integrity will be ensured through the following of the proper maintenance procedures on databases and through timely upgrades of the database software to current releases.

A naming standard must be in effect to distinguish between test jobs and production jobs, test data sets and production data sets. New procedures should be run in test data sets and off-line data sets.

Employees are charged with safeguarding the integrity, accuracy, and confidentiality of information.

F. Backup and Storage
Data will be secured against loss by regular backing up of the data onto removable media. Data centers may have a fireproof and weatherproof vault for critical electronic data storage such as backup media (tapes, removable disks).

See Board Policy 8300