DCC Information Security Standards

Added by Lorraine Messina, last edited by Klaus Gessler on Apr 03, 2013

DCC Information Security Standards

Information security is the responsibility of EVERYONE who has access to information contained in college administrative systems. That information may reside on computer systems or on paper reports

The protection of DCC student and employee information is REQUIRED BY LAW

The college must adhere to Federal Family Educational Rights and Privacy Act (FERPA) and Health Insurance and Portability and Accountability Act (HIPAA) laws.
New York State requires the college to adhere to a minimum set of information security standards. The NYS policy can be viewed in myDCC on the Working@DCC tab.

What data is confidential?

- Information maintained in college administrative systems should be assumed to be confidential unless otherwise specified.
- MOST personal student and employee data is confidential and must be protected.
- Only directory information is considered public information. Directory information is limited to: Name, Email, Dates of attendance, Date of graduation, Degree Enrollment status.

> ⚠ A student may submit a waiver prohibiting the college from releasing his/her directory information, so even releasing directory information requires judgment

Employees are responsible for understanding and complying with policies regarding to access, and the secure disposal of information they have access to.

- Staff employees should discuss and review policies with their supervisor.
- Faculty should review policies with the Office of Academic Affairs.
- College policies can be viewed from the Working@DCC tab on myDCC by selecting the Campus Documents link. Policies are found under the Technology and Security Documents heading.

Employees should raise an alarm if they think information is not being properly handled. They should notify their supervisor or the Associate Dean of Information Technology.

Employees are accountable for their actions.

Employees should have no expectation of privacy regarding the information stored on college computer systems.

Information Security Best Practices

- NEVER release information over the phone unless you can positively confirm the identity of the caller.
- Be vigilant and protect access to your computer account - NEVER allow ANYONE to use your computer account and password
- NEVER download college data to laptops or removable storage (CDs, diskettes or flash drives).
- Be sure records on your desk cannot be viewed by the public. Always keep reports an arm¿s length away from public areas.
- ALWAYS keep reports locked up when not in use.
- ALWAYS shred or discard in secure disposal containers any forms and printouts with student information