

## **Information Security Awareness for New Faculty and Staff Policy**

*Approved by Senior Administrators, May 22, 2006*

*Updated: December 9, 2010*

### **Policy**

Connecticut College faculty and staff should understand the importance of information security and endeavor to protect college-owned and personal computers and electronic information. To facilitate appropriate information security practices, all new Connecticut College faculty and new and current staff members who use campus or college-owned computer resources or networks must complete an Information Security Awareness Orientation class that offers information security education that addresses how to protect college and personal electronic information. Current employees who have not completed the information security awareness orientation class will be limited to Banner Self-Service on the Banner administrative system and may have network access suspended.

In addition, those permanent employees who have access to Personal Information, as defined below, are required to participate in a Personal Information Security Training program at least once per year. All temporary employees who have access to Personal Information must undergo security awareness training before they can access the personal information. The training program shall cover the requirements of the “Storage, Access, and Transmission of Confidential and Personal Information Policy” (December 2010). Any employee with access to Personal Information who fails to participate in the required training may have network access suspended.

For the purpose of this policy, “Personal Information” means:

- (i) information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number;
- (ii) students’ “education records” under FERPA, which - with limited exceptions - means all records in any format or medium that are directly related to a student and are maintained by the College;
- (iii) protected health information as defined by HIPAA, which generally includes identifiable health information – with certain exceptions; and
- (iv) nonpublic personal information as defined by GLB.

Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. Personal Information includes information stored in any format, including but not limited to electronic media, hard copy documents, and certain types of information that may be conveyed orally. Any employee with questions about whether certain information constitutes Personal Information as defined by this policy or

any other question about the meaning or implementation of this policy should contact the Office of the Vice President for Information Services.

Employees who do not comply with this policy may be subject to disciplinary action, including but not limited to, termination.