SUNY Cortland Information Resources Unit - Confidentiality Policy and Procedures
August 18, 2010

Policy Summary:
SUNY Cortland's Information Resources (IR) Unit and its reporting departments (academic computing/classroom media services, administrative computing, , memorial library, and networking and telecommunications) places significant value on its ability to establish trust and credibility among its constituents. A critical aspect of IR's responsibilities is to provide support and maintenance of the College's information resources systems. This requires IR staff to occasionally access employee and student password protected electronic information as well as computer hard drives and other peripheral devices. . This support includes, but is not limited to, employee or student assistance requests, software and network upgrades, responses to emergency vulnerabilities and virus attacks, and providing assistance to human resource and/or university police investigations. In performing these responsibilities, IR staff may have access to personal, confidential and sensitive information. It is critical that this access be restricted according to the rules and procedures outlined below and that any information to which IR staff is privy is held in confidence and only used for legitimate College purposes.

Rules and Procedures:
SUNY Cortland's Information Resources staff shall:

1. Maintain strict confidentiality requirements and regulations in compliance with the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act of 1974 as amended (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and New York State's Personal Privacy Protection Law (Public Officers Law, Article 6-A) in addition to other federal and state laws which may become applicable. These laws pertain to the security and privacy of all non-public information including student information, employee information, and general College information whether it is in hard copy or electronic form.
2. Protect against unauthorized access of such information as detailed in number one above, ensure the security and privacy of such information, and disclose any anticipated threats or hazards that may compromise the confidentiality of such information to the SUNY Cortland Information Security Officer.
3. Not release this information to the public, including but not limited to co-workers who have not been authorized or who do not have a legitimate business/educational need to know. Any questions regarding release of such information to another person will be directed to the respective director or the Associate Provost for Information Resources.

Unauthorized access and use shall be defined as:

1. Access to student, employee, or College information which is not necessary to carry out assigned job responsibilities. This includes, but is not limited to, reviewing files, data, email, voice mail, internet sites, desk drawers, or anything else that is not directly related to the task being completed.
2. Access to the records of a student or employee for which signed authorization has not been obtained. This includes children of faculty/staff (protected under FERPA), spouses, parents, and other relatives.
3. Release of student or employee information to unauthorized internal or external users.

4. Release of more student or employee information to an authorized individual/agency than is essential for meeting the stated purpose of an approved request.
5. Disclosure of the IR staff member's system username, password, or access codes to an unauthorized individual.

Furthermore, electronic information accessed may not be divulged, copied, released, sold, loaned, reviewed, altered or destroyed except as properly authorized as noted in the next section..

Authorized access procedures and responsibilities:

1. Whenever possible, computer support will be pre-arranged to occur in the presence of the user, whether in person or through remote access.
2. Employee requests for new and/or upgraded hardware or software utilizing the Information Resources request forms shall constitute consent for access to install the requested item(s).
3. Employee requests for assistance through the Information Resources Support Center which result in the issuance of a trouble ticket shall constitute consent for access to troubleshoot and/or fix the reported problem.
4. Any access to electronic information when the user is not present or without direct consent of the user will only occur upon direct authorization. Direct authorization may be given by one of the following individuals and will be confirmed in writing, which may occur via email:
    - Director, Academic Computing
    - Director, Administrative Computing
    - Director, Library
    - Director, Networking and Telecommunications
    - Associate Provost for Information Resources
    - Provost and Vice President for Academic Affairs
    - Assistant Vice President for Human Resources
    - Associate Director of Human Resources
    - University Police Chief or Assistant Chief

IR staff will be held responsible for the misuse or wrongful disclosure of confidential, sensitive, and/or private information. Furthermore, IR staff shall abide by the rules, regulations, policies, and procedures of SUNY Cortland as well as federal and state laws applicable to his/her position at the College. The obligation to maintain the confidentiality of all SUNY Cortland non-public confidential information will continue after termination of employment.

Additionally, failure to comply with the SUNY Cortland Information Resources Unit Confidentiality Policy and Procedures statement may result in legal and/or disciplinary actions. Disciplinary actions, consistent with the appropriate collective bargaining agreement, may include termination of employment, regardless of whether criminal or civil penalties are imposed, depending upon the nature and severity of the breach of confidentiality.

Related Links:

Family Educational Rights and Privacy Act http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Gramm-Leach Bliley Act http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
Health Insurance Portability and Accountability Act http://www.hhs.gov/ocr/privacy/
NYS Personal Privacy Protection Law http://www.dos.state.ny.us/coog/actualpppl.html