Establishing and Maintaining an Information Security Program

The Gramm-Leach-Bliley Act (Public Law 106-102) provides consumers the right to the protection of their nonpublic Personally Identifiable Information (PII) and requires financial institutions possessing such information about consumers to publish a privacy policy. This policy is published on the CSI website and a notice of the web location is published in the Academic Catalog. A notice of the location of this policy is also provided annually to students.

General Privacy Policy: CSI carefully protects all nonpublic personal information in our possession regarding students and their families. The School will not release nonpublic, private, personal, or financial information about our students or applicants to any third party, except as specifically provided in this policy. The School will release certain nonpublic personal information to federal and state agencies, government contractors, student loan providers/servicers, and other parties as necessary for the administration of the federal student aid programs, for enforcement purposes, for litigation, and for use in connection with audits or other investigations. Disclosure is permitted to law enforcement or emergency services agencies in the performance of their duties or when student safety or health may be in jeopardy. The School will not sell or otherwise make available personal information for marketing purposes to any third party at any time.

Protection of Personally Identifiable Information: The School employs office procedures and password-protected computer systems to ensure the security of paper and electronic records. The School does not disclose specifics of its internal security procedures to students or the general public to protect the effectiveness of those procedures.

Access to social security numbers and other Personally Identifiable Information (PII) is strictly limited to those School Officials with a need-to-know. Each department director is responsible for enforcement of this policy with regard to the information within his/her office. The Campus President will be responsible for overall control of information release and will resolve any disagreements and make final decisions as necessary in accordance with this Policy.

Computer Systems Institute's information is an important asset that is critical to providing an effective and comprehensive learning environment, openly communicating ideas, providing outstanding community service, and supporting the college's operations. This information includes sensitive and personal student, faculty, and staff data as well as the college's operational data. To maintain effectiveness and protect individuals, the college's information assets must be protected from misuse, unavailability, destruction, and unauthorized disclosure or modification.

The executive leadership of Computer Systems Institute is committed to protecting the value of the college's information assets. The IT Department is charged with establishing and maintaining a program that preserves the confidentiality, integrity, and availability of information and information systems. This responsibility is addressed by:

Continually assessing risks and defining appropriate protection strategies

Complying with applicable legal and regulatory requirements

Protecting the reputation, image and competitive advantage of the college

Supporting Computer Systems Institute's strategic mission and goals

Maintaining partnership with administrative units, faculty, and staff to ensure a collaborative approach to information security

The IT Department deals with numerous threats and challenges including data loss or theft, malicious software (e.g., viruses, worms, Trojan horses), identity theft, social engineering, phishing scams, and risks associated with

new technologies. Security measures also must be implemented to comply with several laws and regulations that address student information (FERPA), financial information, individuals' privacy data and individuals' health information.

The IT Department offers a wide range of products and services to address information security risks and requirements. These offerings are designed to balance strategic, tactical, and operational needs, and they include the following specific products and services:

Security policies, procedures, standards, and methodologies

Security awareness and training

Legal and regulatory compliance

Security strategy, architecture, and technologies (including technologies to protect against malicious software)

Technical system configurations and vulnerability management

Response to information security incidents or breaches

Security requirements for software development and acquisition

Disaster recovery and continuity planning

Policies and procedures provide the foundation of an effective information security program and define minimum requirements for protection of information. The IT Department of Computer Systems Institute has developed and implemented policies that specify appropriate controls and conduct. These policies have been approved by the college's senior executives, are applicable to all faculty, staff, and students, and they are required to be followed. They are available for review in the Computer Systems Institute Policy Manual.

Any suspected information security breach or issue should be reported immediately to the IT Department.