Student Information Security Policy

Coyne College GLBA Required Information Security Overview:

Coyne College follows a comprehensive written Information Security Plan mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). In particular, this document addresses the following plan elements:

(i) ensure the security and confidentiality of covered records,
(ii) protect against any anticipated threats or hazards to the security of such records, and
(iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers.

The Information Security Plan incorporates the Institution's policies and procedures enumerated below and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations.

Designation of Representatives: The President is responsible for coordinating and overseeing the plan elements. In addition, the Executive Management team, IT Technician, and Third-Party IT Managed Services Provider, CTI, are directly involved with all decisions regarding oversight of the plan. Any questions regarding the implementation of the Student Information Security Policy or the interpretation of this document should be directed to the President.

Scope of this policy: The policy applies to any record containing nonpublic financial or health information about a student, employee or other third party who has a relationship with the Institution, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial or health information shall mean any information.

(i) a student, employee or other third party provides to obtain a financial or health service from the Institution,
(ii) about a student, employee or other third party resulting from any transaction with the Institution involving a financial or health service, or
(iii) otherwise obtained about a student, employee or other third party in connection with providing a financial or health service to that person.

Elements of the Student Information Security Policy:

1. Risk Identification and Assessment. The Institution intends, as part of the plan, to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information. In implementing this plan, the President and Executive Management Team (EMT) will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

   - *Employee training and management*. The President and EMT will evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of, including but not limited to, student and/or employee records, including financial aid and health information. This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area, including compliance with external compliance requirements (ex: FERPA, HIPPA, etc.).
   - *Information Systems and Information Processing and Disposal*. The President will coordinate with the EMT, IT Technician, and MSP to assess the risks to nonpublic financial information associated with the Institution's information systems, including network and software design, information processing, and the storage, transmission, and disposal of nonpublic financial information. This evaluation will include assessing CC's current policies and procedures (ex: Use of Computers, Record Retention, etc.). The MSP will assess procedures for monitoring potential information security threats associated with software systems and for updating such systems (ex: implementing patches or other software fixes designed to deal with known security flaws, etc.).
   - *Detecting, Preventing and Responding to Attacks.* The IT Technician and EMT will coordinate with the MSP, CTI, to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks.

2. Designing and Implementing Safeguards**.** The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other forms. CTI will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The IT Technician and President shall coordinate with those responsible for the third party service procurement activities among the Information Services and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the President will work with the EMT to identify contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards.

4. Adjustments to Policy**.** The President is responsible for evaluating and adjusting the policy based on the risk identification and assessment activities undertaken pursuant to the policy, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the policy.

Procedures for Reporting a Breach: In the event of a security breach or a suspected security breach Coyne College will notify the Department of Education the same day Coyne College is aware that there has been a security breach**.**

Contact(s): Russell T. Freeman, President

December 3, 2020