2175 – Barton Community College GLBA Required Information Security

Overview: This document summarizes Barton Community College's comprehensive written Information Security Program mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). In particular, this document describes the Progam elements pursuant to which the Institution intends to (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 Program incorporates by reference 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, including, without limitation, FERPA, HIPAA, GLBA, GDPR, FTC – Red Flag Policies.

Designation of Representatives: Barton's Chief Information Officer, is designated as the Chief Information Security Officer (CISO) who shall be responsible for coordinating and overseeing the Program. The Program Officer (CISO) may designate other representatives of the Institution to oversee and coordinate particular elements of the Program. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the CISO or his or her designees.

Scope of Program: The Program 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 in order 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 Program:

1. Risk Identification and Assessment. The Institution intends, as part of the Program, to undertake 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 the Program, the CISO will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- *Employee training and management*. The CISO will coordinate with Barton representatives to 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 requirements resulting from the following external provisions:

    - Family ~~Familty~~ Educational Rights & Privacy Act (FERPA)
    - Health Insurance ~~Information~~ Portability & Accountability Act (HIPAA)
    - Federal Trade Commission – Red Flag Policies

- General Data Protection Regulation (GDPR)
- Gramm-Leach-Bliley ~~Blibley~~ Act (GLBA)

- *Information Systems and Information Processing and Disposal.* The CISO will coordinate with representatives of the Barton's Information Services 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 Barton's current polices and procedures relating to the following:

  - Policy 1110; Procedure 2111 Use of Computers/College Computing and Information Systems
  - Policy 1110; Procedure 2111A Individual Email Policy [link to come soon after approval]
  - Policy 1166; Procedure 2150 Use of Copyright Materials
  - Policy 1170; Procedure 2170 Record Retention

  The CISO will also coordinate with Barton's Information Services to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- *Detecting, Preventing and Responding to Attacks*. The CISO will coordinate with Barton's Information Services 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 and developing incident response teams and policies. In this regard, the CISO may elect to delegate to a representative of the Information Services the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Institution.

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. The CISO 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 CISO 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 CISO will work with the Vice President of Administration to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Vice President of Administration. These standards shall apply to all existing and future contracts entered into with such third party service providers, provided that amendments to contracts entered into prior to June 24, 2002 are not required to be effective until May 2004.

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

Contact(s): Chief Information Officer

Related Form(s):

References: NACUBO GLBA Template

Relevant Policy or Procedure(s): Policy 1110 – Use of Computers/College Computing and Information Systems; Procedure 2111 Use of Computers/College Computing and Information Systems; Procedure 2111A Individual Email Policy [link to come soon after approval]; Policy 1166 – Copyright Law; Procedure 2150 Use of Copyright Materials; Policy 1170 – College Record Retention and Security; Procedure 2170 Record Retention

Approved by: President

Date:

Revision(s):