Name:	**Gramm-Leach-Bliley Act (GLBA) Safeguards Policy**
Category:	Administrative
Subject:	Information Security
Owner:	Information and Instructional Technology
Related Procedures:	N/A
Related Forms:	N/A

I. SCOPE

This document summarizes the Delaware Technical Community College (hereafter College) comprehensive written information security program mandated by the Federal Trade Commission's Safeguards Rule and the Gramm-Leach-Bliley Act (GLBA). The goals of this program are as follows:

- To ensure employees have access only to the relevant data needed to conduct College business;
- Protect against anticipated threats to the security or integrity of customer records and information;
- To safeguard and prevent unauthorized access to personally identifiable financial records and information maintained by the College;
- To comply with existing College policies, standards, guidelines, and procedures; and
- To comply with applicable federal, state, and local regulations.

II. POLICY STATEMENT

Delaware Technical Community College will protect, to the extent reasonably possible, the privacy, security, and confidentiality of personally identifiable financial records and information. This policy applies to all personally identifiable financial records and information and covers employees and all other individuals or entities using these records and information for any reason. This policy also establishes an expectation that members of the College community act in accordance with this policy, relevant laws, contractual obligations, and the highest standards of ethics.

III. POLICY

Definitions

The following definitions apply to this policy:

Customer: an individual who has obtained a financial product or service from the College to be used primarily for personal, family, or household purposes, and who has a continuing relationship with the College. Examples of activities which create customer relationships with the College could include obtaining a loan from the College or having a loan for which the College has servicing rights or responsibility.

Customer Information: non-public personal information about an individual who has obtained a financial product or service from the College for personal, family or household reasons, that results in a continuing relationship with the College. Examples would be any extension of credit by the College for household, personal or family purposes, such as an extension of credit for tuition, fees, housing, medical services, etc.; the making and/or servicing of loans and/or financial aid. These situations are subject to GLBA, even if the individual ultimately is not awarded any financial aid or provided with a credit extension, in which case their non-public personal information would still be protected under GLBA.

Financial Service: defined by federal law to include, but not be limited to, such activities as the lending of money; investing for others; providing or underwriting insurance; giving financial, investment or economic advisory services; marketing securities and the like.

Information Security Program or Program: a program developed, maintained, and enforced by the office of the vice president for information and instructional technology in accordance with the Federal Trade Commission's Safeguards Rule and the Gramm-Leach-Bliley Act to ensure that the information assets of the College are maintained securely.

Nonpublic Financial Information: shall mean any information (i) a student or other third party provides in order to obtain a financial service from the College, (ii) about a student or other third party resulting from any transaction with the College involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Service Provider: any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its direct provision of services to the College.

Responsibility(ies)

Delaware Technical Community College's vice president for information and instructional technology (IIT) is the designated Information Security Program (ISP) Coordinator. The ISP is responsible for directing and overseeing the information security program. The ISP may designate other representatives of the College to oversee and coordinate particular elements of the information security program. Any questions regarding implementation or the interpretation of this document should be directed to the ISP or their designees.

Procedure

1. Employee Responsibilities and Access:
   The following restrictions apply to all personally identifiable financial records and information maintained by the College and are meant to safeguard the security of these records and to maximize the integrity of the information. College employees are responsible for ensuring that, within their areas of responsibility, appropriate enforcement of this program will be maintained.

- College employees are granted access to those data and information resources required to carry out the responsibilities of their position and may not access additional resources without authorization (in other words, employees may not access customer information unless they have a need to know that information to perform their job duties).
- Access is determined based on the duties and responsibilities of each position and each employee is responsible for protecting their means of access from misuse (e.g., employees must not share their username/password(s) with anyone else, or allow others to have access to their keys, etc.).
- Employees shall not knowingly alter, destroy, or misuse customer information.
- Employees must ensure that any release of customer information is conducted in an appropriate and secure manner (e.g., employees should not release customer information without verifying the identity of the person(s) requesting the information; employees should use password protected file attachments and/or encrypted emails when transmitting confidential information, etc.).

2. Program Administration:
    a. *Risk Identification and Assessment.* Delaware Technical Community College will, as part of the information security program, annually 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 information security program, the ISP or their designee will establish procedures for identifying and assessing such risks in each relevant area of the College's operations, including:
        - *Employee training and management.* The ISP will coordinate with Delaware Technical Community College representatives to evaluate the effectiveness of the College's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of College's current policies and procedures in this area, including compliance requirements resulting from the following external provisions:
            - Family Educational Rights & Privacy Act (FERPA)
            - Health Insurance Portability & Accountability Act (HIPAA)
            - General Data Protection Regulation (GDPR)
            - Gramm-Leach-Bliley Act (GLBA)
        - *Information Systems and Information Processing and Disposal.* The ISP will coordinate with representatives from Information and Instructional Technology to assess the risks to nonpublic financial information associated with the College's information systems, including network and software design, information processing, and the storage, transmission, and disposal of nonpublic financial information. The ISP will also

coordinate with the College's information security officer (ISO) to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, implementing patches or other software fixes designed to deal with known security vulnerabilities.

- *Detecting, Preventing and Responding to Attack.* The ISP and/or their designee will 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. The ISP may elect to delegate to information security personnel 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 Delaware Technical Community College.

b. *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 ISP 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.

c. *Overseeing Service Providers.* The ISP or their designee shall coordinate with those responsible for the third-party service procurement activities 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 ISP will work with the divisions of Legal Affairs and Finance 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 College's general counsel.

d. *Adjustments to Program.* The ISP 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 College's operations or other circumstances that may have a material impact on the program.

Exceptions

Any exceptions to this program must be approved by the president upon the recommendation of the vice president for information and instructional technology. Questions regarding this program should be referred to the College's general counsel.

IV. EFFECTIVE DATE(S)

This policy is effective on the date of approval.

V. FREQUENCY OF REVIEW AND UPDATE

This policy will be reviewed and updated annually.

VI. SIGNATURE AND DATE OF APPROVAL

Mark T. Brainard, President — Date