Danville Area Community College #507
Information Security Plan

I. Purpose

In order to protect private information and data, and to comply with the Federal Law, known as Gramm-Leach-Bliley Act (GLB Act), Danville Area Community College has adopted this Information Security Plan for certain highly critical and private financial and related information. This security plan applies to customer financial information ("covered data") the College receives in the course of business. The document describes how the College 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 of information in ways that could result in substantial harm or inconvenience to customers. This Plan 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, and HIPAA. The practices in the document will be carried out by and impact diverse areas of the College.

II. Gramm Leach Bliley Act Requirements

The Financial Services Modernization Act of 1999, also known as Gramm Leach Bliley Act (GLB Act) 15 U.S.C. #6801, mandates that the College appoint an Information Security Plan Coordinator, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

III. Definitions

"Covered Data" means all information required to be protected under the GLB Act. The data includes information obtained from a customer and employee in the course of offering a financial product or service, or such information provided to the College from another institution. Examples of financial information relating to such products or services are bank and credit card account numbers, income and credit histories, social security numbers, student loan information, income tax information from a current or prospective student as a part of a financial aid application, and billing account financial information. Covered data consists of both paper and electronic records that are handled by the College or its affiliates.

"Service Providers" refers to all third parties who, in the ordinary course of College business, are provided access to covered data. Service providers may include business retained to transport and dispose of covered data, collection agencies, tuition payment plan companies, student loan servicers, banks, and systems support providers, for example.

IV. Information Security Plan Coordinator

The Facilitator(s) of the College's Information Security Team (the Team) is designated as the Information Security Plan Coordinator(s). The Team shall be responsible for coordinating and overseeing the Plan. This individual(s) will work closely with the Team which will include at a minimum, the Director of Computer Network and End User Services, Director of Administrative Data Systems, Controller, Vice President of Finance/Chief Financial Officer,

Director of Admissions and Records/Registrar, Director of Financial Aid, Vice Presdient of Human Resources, and Dean of Student Services, to accomplish this mission. Other relevant academic and administrative departments throughout the College may also be involved.

V. Elements of the Plan:

1. Risk Identification and Assessment

The Information Security Plan will identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise such information, and assess the sufficiency of any safeguards in place to control these risks. Risk assessments will include consideration of risks in each area that has access to covered information. Risk assessments will include, but not be limited to consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal, and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures.

The Team will work with all relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks, as well as risks unique to each area with covered data. Risk assessments should be conducted periodically. The Team may identify a responsible party in each department with access to covered data to conduct the risk assessment considering the factors set forth above, or employ other reasonable means to identity risks to the security, confidentiality and integrity of covered data in each area of the College with covered data.

DACC recognizes that it has both internal and external risks. These risks include but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

2. Employee Training and Education

While director and supervisors are ultimately responsible for ensuring compliance with information security practices, The Team, will work in cooperation with the Office of Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all university data; custodians of covered data; and those employees who use the data as part of their essential job duties.

3. Information Systems and Information Processing and Disposal
The Team will work with the Computer Network and End User Services' staff and the Administrative Data Systems staff to assess the risks to covered data associated with the College's information system, including network and software design, information processing, and the storage, transmission, and disposal of nonpublic financial information. This evaluation will include assessing the Institution's current polices and procedures relating to acceptable use of the institution's network and network security, document retention and destruction. It will also include assessing 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.

4. Detecting Preventing and Responding to Attacks
The Team will delegate to the Computer Network and End User Services' staff and the Administrative Data Systems staff the responsibility of evaluating 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.

VI. Oversight of Service Providers and Contracts
GLB requires the College to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. The Team shall coordinate with those responsible for third party service procurement activities 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. The Team may need to work with Legal Counsel to develop and incorporate standard, contractual protections applicable to third party service providers which will require such providers to implement and maintain appropriate safeguards.

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

Adopted: 2-5-2005

Revised: 10-13-2017