POLICY: 7004 Federal Personal Information Security Programs

BOARD POLICY

Identity Theft Prevention Program

The Board recognizes the importance of identity theft prevention. The Board also recognizes that the Colleges currently maintain certain "covered accounts" as defined by the Federal Trade Commission (FTC) that include loan programs and payment plans. In response to the FTC's issuance of "Red Flag Rules", each College will establish and maintain an Identity Theft Prevention Program that includes identification, detection, prevention and mitigation of identity theft risks. The programs should be periodically reviewed and updated to consider changes to the plan in response to the changing environment.

A Red Flag, as included in the FTC's rules, and also included below, is defined as a relevant indicator of a possible risk of identity theft. The Identity Theft Program should include, at a minimum, the following sections:

1) Identification
   In identifying Red Flags, each College should consider the types of covered accounts it offers and maintains, the methods it provides to open and access its covered accounts, and its previous experiences with identity theft.

2) Detection and Prevention
   Each program should include consideration of the detection of Red Flags in connection with the covered accounts. The program should also include obtaining identifying information about, and verifying the identity of, a person opening a covered account. This information should then be used to authenticate customers, monitor transactions, and verify the validity of change of address requests.

3) Response
   Each program should provide for appropriate responses to detected Red Flags to prevent and mitigate identity theft.

Each program should be reviewed and updated periodically to reflect changes in risks such as:

*experiences with identity theft
*changes in methods of identity theft
*changes in methods to detect, prevent, and mitigate identity theft
*changes in service provider arrangements

Each College shall submit its initial Identity Theft Program for approval by the Board. Thereafter, a copy of each College's current program and annual report on compliance shall be kept on file at each College. Each College President, or designee, will be responsible for oversight of the Identity Theft Program at their college.

Customer Information Security Program

The Board recognizes the importance of protecting non-public student financial information. The Board further recognizes that by virtue of the Colleges' participation in the Title IV Federal student financial aid programs authorized under Title IV of the Higher Education Act, each College is subject to certain requirements of the Gramm Leach Bliley Act (GLBA).

The Board directs each College to develop an Information Security Program to protect non-public financial information consistent with the following policy.

Each College must identify and periodically assess external and internal risks to the security, confidentiality, and integrity of non-public financial information. These risks may include:

- Unauthorized access to information by individuals other than employees with a legitimate purpose for viewing such information;
- Breaches of computer network security resulting in unauthorized access or transfer of information to third parties;
- Physical loss of data resulting from fire, flood or other disaster;
- Unauthorized requests and releases of information to third parties; and
- Unauthorized access through hardcopy files or reports.

Each College must establish a written plan and procedures to manage and control the risks. The plan and procedures must specifically address information gathered and maintained through College computer systems and in all physical files. Additionally, the plan must provide for the training of employees regarding the importance of confidentiality of student records, student financial information, and other types of non-public data and information. The plan and procedures shall be periodically reviewed and updated in order to address changes in risks, technology or the sensitivity of the information.

Each College President shall designate an individual responsible for the development, implementation, and periodic review of the plan and procedures. Each College must submit its written plan and procedures to the System Office and maintain a current copy on file along with a record of the periodic reviews of the plan and procedures.

Policy Adopted: 1/13/09
Policy Revised: 3/24/17