Purpose

The purpose of this procedure is to establish protocols and guidelines required by the College's Identity Theft Program. The procedures identified must be consistent with Florida Statute and ensure compliance with the Federal Trade Commission (FTC) Red Flags Rule and College Board Rule.

Procedure

A. Scope and general guidelines:

1. "Covered Account" is a consumer account that involves multiple payments or transactions, such as a loan or payment plan that is billed or payable on a future date, or multiple payments in arrears, in which a "continuing relationship" is established or any other account for which there is a reasonably foreseeable risk from identity theft.

2. A "Red flag" is a pattern, practice, or specific activity that could indicate identity theft.

3. The College is considered a "creditor" under the Red Flags Rule because it allows students to register now and pay on a future due date and offers institutional payment plans to students.

B. Responsibilities and delegation of authority:

1. College employees will use these procedures to identify when new or existing billing accounts are opened using false information, protect against the establishment of false student accounts, ensure existing accounts are not opened using false information, and to report potential identity theft.

2. The Associate Vice President of Finance is responsible for the oversight of the Program.

3. The College Bursar will develop, implement, and administer the program as approved by the Associate Vice President of Finance.

4. The Bursar will review the program at least annually, or after each and every attempt at identity theft. A report will be prepared annually and submitted to the Associate Vice President of Finance to include matters related to the program, the effectiveness of the policies and procedures, a summary of any identity theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

5. Service providers with access to the College's covered account data must contractually agree to have policies, procedures and programs that comply with the FTC Red Flag Rule. In addition, service providers must notify the College of any security incidents that may compromise the College's covered account data.

C. Identifying Red Flags:

1. The College adopts the following red flags to detect potential fraud:

   a. Notice of credit freeze provided by credit reporting agency.
   b. Notice of address discrepancy provided by consumer reporting agency.
   c. Identification documents appear to be altered.
   d. Photo and physical description do not match appearance of applicant.
   e. Other information is inconsistent with information provided by applicant.
   f. Other information provided by applicant is inconsistent with information on file.
   g. Application appears altered or destroyed and reassembled.
   h. Personal information provided by applicant does not match other sources of information. For example, Social Security Number (SSN) is not a valid number or listed as assigned to a deceased person.
   i. There is a lack of correlation between the social security range and date of birth.
   j. Information provided is associated with known fraudulent activity. The address or phone number provided is the same as one used in a prior fraudulent activity.
   k. Information commonly associated with fraudulent activity is provided by applicant. Examples include an address which is a mail drop or prison, and a non-working phone number that is associated with an answering service or pager.
   l. The Social Security Number, address, or telephone number is the same as that of other applicants of the College.
   m. Applicant fails to provide all information requested.
   n. Personal information provided is inconsistent with information on file for applicant.

2. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

D. Response to attempted or suspected fraudulent use of identity:

1. Internal Notification - Any College employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer identity must notify the Campus Director of Administrative Services and the Bursar.

2. External Notification - The College shall notify the affected individual(s), if possible, of any actual identity theft. The following information will be included in the notice:

   a. General information about the incident.
   b. The type of identifying information involved.
   c. The College telephone number that the affected individual can call for further information and assistance.
   d. The local Law Enforcement Agency with proper jurisdiction.

e. The Federal Trade Commission (FTC) Telephone number: 877-438-4338 and the FTC ID Theft website.
f. Advise affected individual to place fraud alerts on their credit reports by contacting the credit reporting agencies.

3. Method of Contact - Written notice shall be sent certified mail to last known "good address" if identity theft involves alteration of the correct address of record. The College will telephone the individual provided the contact is made directly with the verified, affected person and appropriately documented.

4. Local Law Enforcement - In all cases, the College will notify the General Counsel and local law enforcement having proper jurisdiction of any incident of actual identity theft.

E. Employee training and review:

1. The College will implement periodic training to emphasize the importance of meaningful data security practices and to create a culture of awareness and security.

2. The College acknowledges that a well-trained workforce is the best defense against identity theft and data breaches.

a. The program rules will be explained to relevant staff on an annual basis. Staff will be trained to spot security vulnerabilities and will be updated about new risks and vulnerabilities.
b. Employees will be trained about the importance of safeguarding confidential information, FERPA guidelines, and the ethical policies of the College.
c. Employees will be advised that violation of this policy is grounds for discipline, up to and including dismissal.

REFERENCES: 15 USC § 6805, 16 CFR § 314.3, FS 817.02, 817.568, 1001.64, 1001.65

Adopted Date: September 7, 2010
Revision Date: January 14, 2014, December 13, 2016