**PENSACOLA STATE COLLEGE**
MANUAL OF PROCEDURES

| Procedure Title: | Identity Theft Prevention Program | Number 140 |
|---|---|---|
| Related Policy: | Identity Theft Prevention Program – 6Hx20-1.037 | Page Page 1 of 4 |

## I. Purpose

To identify third party arrangements and "Red Flags" that will alert appropriate College officials on behalf of employees and students when new or existing billing accounts are opened using false information and measures to respond to such events. Within the context of this procedure, "Red Flags" mean patterns, practices, or specific activities that indicate the possible existence of identity theft.

This procedure applies to Covered Accounts, credit report usage, and third party service arrangements within the Identity Theft Red Flags Rule as promulgated by the Federal Trade Commission.

## II. Procedure

A. General Guidelines

1. Covered Accounts under the Red Flags Rule are consumer accounts that involve multiple payments or transactions, such as loans that are billed or payable monthly, or multiple payments in arrears, in which continuing relationships are established. Certain payment arrangements, such as payment of tuition in full at the beginning of each semester either by the student's family or through a third-party student loan provider, does not meet the continuing relationship standard in the Covered Accounts definition.
2. The College is considered a creditor under the Red Flags Rule because it offers institutional loans to students.
3. The procedure also applies when the College uses consumer reports to conduct background checks on prospective employees.

B. Responsibilities and Delegation of Authority

The Vice President, Business Affairs, is responsible for the oversight of the Identity Theft Prevention Program ("Program").

C. Internal Risk Assessment

1. The College will conduct an internal risk assessment to evaluate how at risk the current procedures are at allowing students to create a fraudulent account and evaluate if current (existing) student accounts are being manipulated. This risk

assessment will evaluate: 1) how new accounts are opened, 2) the methods used to access the account information, and 3) third party service arrangements. Using this information the College will be able to identify areas of highest risk for review and compliance.

a. New accounts opened in person;
b. New accounts opened via the world wide web;
c. Account information accessed in person;
d. Account information accessed via telephone;
e. Account information accessed via the world wide web; and
f. Delinquent accounts placed with an outside collection agency.

2. Oversight of Third Party Services Providers:
The College will, as part of its contracts with third party service providers (e.g., collection agencies and tuition payment plans), require that providers have policies, procedures, and programs that comply with the Red Flags Rule. Further, service providers must notify the College of any security incident they experience, even if the incident may not have led to an actual compromise of the College's applicant data.

D. Identifying Red Flags

The College adopts the following Red Flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary:

1. Fraud or active duty alerts included with consumer reports;
2. Notice of address discrepancy provided by a consumer reporting agency;
3. Identification documents appear to be altered;
4. Photo and physical description do not match appearance of applicant;
5. Other information is inconsistent with information provided by applicant;
6. Other information provided by applicant is inconsistent with information on file;
7. Application appears altered or destroyed and reassembled;
8. Personal information provided by applicant does not match other sources of information (e.g., SSN not issued or listed as deceased);
9. Information provided is associated with known fraudulent activity (e.g., address or phone number provided is same as that of prior fraudulent activity);
10. Information commonly associated with fraudulent activity is provided by applicant (e.g., address that is a mail drop or prison, non-working phone number or associated with an answering service or pager);
11. SSN, address, or phone number is the same as that of another applicant at the College;
12. Applicant fails to provide all information requested;
13. Personal information provided is inconsistent with information on file for applicant;
14. Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet; and
15. Identity theft is reported or discovered.

E. Response to Attempted/Suspected Fraudulent Use of Identity

In all cases, the College will notify its Public Safety Department of any attempted or actual identity theft. Employees that may suspect fraud or detect a Red Flag will implement the following response as applicable. All detections or suspicious Red Flags shall be reported to their supervisor and the Vice President, Business Affairs:

1. Internal Notification
   College employees who become aware of a suspected or actual fraudulent use of a customer's or potential customer's identity must notify their supervisor who will then notify the Vice President, Business Affairs.
2. External Notification
   a. Affected Individuals. The College will notify the affected individual(s), if possible, of any actual identity theft. The following information will be included in the notice:
      i. General information about the incident;
      ii. The type of identifying information involved;
      iii. The College phone number that the affected individual can call for further information and assistance;
      iv. The local law enforcement agency with proper jurisdiction;
      v. The Federal Trade Commission phone number and ID theft website: (877) 438-4338, http://www.consumer.gov/idtheft;
      vi. Advise affected individuals to place fraud alerts on their credit reports by contacting the following credit reporting agencies:
         aa. Equifax: (800) 525-6285 or http://www.equifax.com;
         bb. Experian: (800) 397-3742 or http://www.experian.com; and
         cc. TransUnion: (800) 916-8800 or http://www.transunion.com.
   b. Method of Contact. The College will use the following method of contract when notifying the affected individual(s):
      i. A written notice via certified mail to the last known good address if the identity theft involves alteration of a correct address of record; and/or
      ii. A phone call, provided that the contact is made directly with the verified, affected individual and appropriately documented.

F. Employee Training

The College will implement periodic training to emphasize the importance of meaningful data security practices and to create a culture of security. The College acknowledges that a well-trained workforce is the best defense against identity theft and data breaches.

1. Annually, explain the Program rules to relevant staff, and train them to spot security vulnerabilities, and update them about new risks and vulnerabilities.
2. Inform employees of the College's Ethics and Anti-Fraud Policies and Procedures.
3. Inform employees of FERPA Guidelines.
4. Advise employees that violation of the College's security policies is grounds for discipline, up to, and including, dismissal.

G. Identity Theft Prevention Program Review and Approval

The Vice President, Business Affairs, 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 President to include matters related to the Program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

| | |
|---|---|
| Responsible Official | Vice President, Business Affairs |
| President's Signature:  | Date: 02/21/2017 |