PENSACOLA STATE COLLEGE
MANUAL OF PROCEDURES

Procedure Title:	Identity Theft Prevention Program	Number 140
Related Policy:	Identity Theft Prevention Program – 6Hx20-8.002	Page Page 1 of 4

I. Purpose

To reduce the risk of identity theft related to the collection and storage of personal information needed for the College to conduct business and to comply with the Federal Trade Commission (FTC) Red Flags Rule.

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, do 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 overseeing the Identity Theft Prevention Program ("Program"). The Information Security Advisory Team (ISAT) committee will immediately oversee this responsibility, as it has members from all areas of the College, ensuring awareness of all areas incorporated and considered during the regular review.

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 internet.
c. Account information accessed in person.
d. Account information accessed via telephone.
e. Account information accessed via the internet.
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. Furthermore, service providers must notify the College of any security incident they experience, even if the incident does not result in 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. Notifications and Warnings from Credit Reporting Agencies
   a. Fraud or active duty alerts included with consumer reports;
   b. Notice or report from a credit agency of a credit freeze on a customer or applicant;
   c. Notice of address discrepancy provided by a consumer reporting agency; and
   d. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.
2. Suspicious Documents
   a. Identification documents appear to be altered;
   b. Photo and physical description do not match the appearance of applicant;
   c. Other information is inconsistent with information provided by applicant;
   d. Other information provided by the applicant is inconsistent with information on file; and
   e. Application appears altered or destroyed and reassembled.
3. Suspicious Personal Identifying Information
   a. Personal information provided by applicant does not match other sources of information (e.g., SSN not issued or listed as deceased);
   b. Information provided is associated with known fraudulent activity (e.g., address or phone number provided is the same as that of prior fraudulent activity);

c. Information commonly associated with fraudulent activity is provided by the applicant (e.g., an address that is a mail drop or prison, a non-working phone number, or associated with an answering service or pager);
d. SSN, address, or phone number is the same as that of another applicant at the College;
e. Applicant fails to provide all information requested;
f. Personal information provided is inconsistent with information on file for the applicant; and
g. The applicant cannot provide information requested beyond what could commonly be found in a purse or wallet.

4. Suspicious Account Activity or Unusual Use of Account
   a. Change of address for an account followed by a request to change the account holder's name;
   b. Payments stop on an otherwise consistently up-to-date account;
   c. Account used in a way that is not consistent with prior use (e.g., very high activity);
   d. Mail sent to the account holder is repeatedly returned as undeliverable;
   e. Notice to the College that a customer is not receiving mail sent by the College;
   f. Notice to the College that an account has unauthorized activity;
   g. Breach in the College's computer system security; and
   h. Unauthorized access to or use of customer account information.
5. Alerts from Others
   a. 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 who 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 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 effective data security practices and foster a culture of security. The College recognizes that a well-trained workforce is the most effective 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 ISAT Committee will review the Program at least annually and recommend and implement changes to policies, procedures, and technologies in operation to better prevent or detect identity theft.

Responsible Official	Vice President, Business Affairs
President's Signature:	Date: 12/03/2025