I. **PURPOSE & INTENT**

Identity theft is a growing problem nationwide and the University of South Florida System (USF System) must take appropriate steps to limit and protect personal identity information and certain financial accounts that it administers.

Pursuant to the Fair and Accurate Credit Transaction Act of 2003 and those certain “Red Flag Rules” set forth therein, the USF System hereby adopts the procedures and protocols outlined below to more effectively identify so called “red flags” that may indicate the potential for identity theft.

In accordance with USF System governance, the USF System President is charged by the USF System Board of Trustees to approve and implement such policies, procedures and protocols as applicable. As such, the Red Flag Rules apply to the Financial Aid Office, the Controller’s Office and other departments within the USF System that manage financial transactions. The President has designated USF Audit and Compliance, the Controller’s Office, Academic Affairs and the Office of the General Counsel to identify additional areas and departments within the USF System to which the Red Flag Rules may apply. Once a determination is made, the head of the applicable department is charged with informing and training appropriate staff members and administering the obligations of these policies and procedures (Department).

II. **STATEMENT OF POLICY**

The USF System adopts these policies and procedures to help protect employees, students, contractors and the USF System from damages related to the loss or misuse of sensitive identity information.

These policies and procedures enable the USF System to protect existing students and staff, reducing risk from identity fraud, and minimize potential damage to the USF System from fraudulent new accounts. The program will help the USF System:
A. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;

B. Detect risks when they occur in covered accounts;

C. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and

D. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

III. PROCEDURES

The USF System has previously adopted certain System-wide policies that define sensitive information and discuss the proper protocol for using, storing and transmitting such information. These policies are:

- **0-508 Information Security Structure**
- **0-515 Electronic Personal Information**
- **0-516 ID (USF)-SSN Appropriate Use Policy**

All employees within the Department are required to comply with these policies. All employees in the Department should review these policies to ensure that such information is being administered properly. In addition, to the sensitive information discussed in the policies above. The following information should be handled with care and confidentiality:

- **Bank Card Information** – including bank card number, expiration date and/or cardholder name. Note that security codes for bank cards may not be retained by the USF System either in electronic nor paper media.

- **Tax Identification Numbers** – including Social Security numbers, business identification numbers and employer identification numbers.

- **Payroll Information** – including paychecks, paystubs, etc.

- **Medical Information for Any Employee or Student** – including but not limited to doctor names and claims, insurance claims, prescriptions, any related personal medical information.
USF System personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with the Florida Public Records Act and the USF System’s open records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his or her supervisor or the General Counsel’s Office.

IV. ADDITIONAL IDENTITY THEFT PREVENTION PROCEDURES
The USF System has determined that these policies and procedures apply to the Department because the Department maintains and/or administers certain “covered accounts” pursuant to federal legislation.

Employees charged with administering these accounts will become familiar with and comply with the procedures set forth below.

A. Covered Accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

1. Business, personal and household accounts for which there are reasonably foreseeable risks of identity theft; or

2. Business, personal and household accounts for which there are reasonably foreseeable risks to the safety or soundness of the USF System from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. Red Flags

1. The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

   a. Alerts, notifications or warnings from a consumer reporting agency;

   b. A fraud or active duty alert included with a consumer report;

   c. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
d. A notice of address discrepancy from a consumer reporting agency as defined in §334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

2. Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or student, such as:

   a. A recent and significant increase in the volume of inquiries;

   b. An unusual number of recently established credit relationships;

   c. A material change in the use of credit, especially with respect to recently established credit relationships; or

   d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

C. Suspicious documents

1. Documents provided for identification that appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

3. Other information on the identification is not consistent with information provided by the person presenting the identification.

4. Other information on the identification is not consistent with readily accessible information that is on file with the USF System, such as a signature or a recent check.

5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

D. Suspicious personal identifying information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the USF System. For example:
• The address does not match any address in the consumer report;

• The Social Security number (SSN) has not been issued or is listed on the Social Security Administration’s Death Master File; or

• Personal identifying information provided by the student is not consistent with other personal identifying information provided by the student. For example, there is a lack of correlation between the SSN range and date of birth.

2. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the USF System. For example, the address on an application is the same as the address provided on a fraudulent application.

3. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the USF System. For example:

• The address on an application is fictitious, a mail drop, or a prison; or

• The phone number is invalid or is associated with a pager or answering service.

4. The SSN provided is the same as that submitted by other persons.

5. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other students.

6. The student fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

7. Personal identifying information provided is not consistent with personal identifying information that is on file with the USF System.

8. When using security questions (mother’s maiden name, pet’s name, etc.), the student cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
E. Unusual use of, or suspicious activity related to, the covered account

1. Shortly following the notice of a change of address for a covered account, the USF System receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.

3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

   • Nonpayment when there is no history of late or missed payments;

   • A material change in purchasing or usage patterns

4. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

5. Mail sent to the customer or student is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s or student’s covered account.

6. The USF System is notified of unauthorized charges or transactions in connection with a student’s or customer’s covered account.

7. The USF System receives notice from students or customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the USF System.

8. The USF System is notified by a student or customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

V. RESPONDING TO RED FLAGS

A. Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect students and customers and the USF System from damages and loss.
1. Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

2. The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

B. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Upon appropriate consultation, actions may include:

1. Canceling the transaction;

2. Notifying and cooperating with appropriate law enforcement;

3. Determining the extent of the potential fraud and exposure to liability of the USF System; and

4. Notifying the actual customer that fraud has been attempted.

VI. PERIODIC UPDATES TO PLAN

A. At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

B. Periodic reviews will include an assessment of which accounts are covered by the program.

C. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

D. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the USF System and its customers.

VII. APPROPRIATE STAFF AND PERSONNEL TRAINING

A. Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or
personally identifiable information that may constitute a risk to the USF System or its customers.

B. Employees must receive annual training in all elements of this policy.

C. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

*Current Responsible Office: USF System Services

*Refer to the appropriate Responsible Office website for a current name of the Vice President or other Responsible Officer.