SOUTH FLORIDA STATE COLLEGE
ADMINISTRATIVE PROCEDURES

PROCEDURE NO. 2159

TITLE: IDENTITY THEFT PREVENTION PROGRAM

BASED ON POLICY: 2.15 SAFEKEEPING, REPRODUCTION, AND DESTRUCTION OF RECORDS

OFFICE OF PRIMARY RESPONSIBILITY: VICE PRESIDENT FOR ADMINISTRATIVE SERVICES/CHIEF INFORMATION OFFICER

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. To comply with the Federal Trade Commission (FTC) Red Flags Rule.

II. Procedure:

A. Necessity of data collection and storage

1. The college's policy is to collect no personal information about a person unless the person affirmatively chooses to make such information available.

2. If a person chooses to share personal information, the information will only be used for the purposes authorized. However, some of the information may be saved for a designated period of time to comply with the state of Florida's archiving policies. Information will not be disclosed to third parties, or other government agencies, unless required by state or federal law.

3. All documents and electronic communications become public documents unless specifically exempted by the Florida Sunshine laws.

4. When accessing the Web server that hosts the college's domain, www.southflorida.edu, certain client information is automatically collected. This information includes: date and time of access; Internet domain; IP address; Web browser; operating system; and hardware and software configuration data. This information does not include any personally identifiable information, such as name, address, or e-mail, unless deliberately disclosed. Any data collected from client machines is used solely for the purpose of ensuring compatibility with the Web site.

B. Safeguarding of collected data

1. Safeguarding of data stored with the use of technology

    a. Technology usage guidelines – Summarize the user responsibilities and support functions that are acceptable at South Florida State College (SFSC). The guidelines include a security awareness program and indicate how data is to be used and stored. A user, either student or employee, cannot obtain a user id without signing an acknowledgment that they have read and understand the data guidelines.

    b. Technology support manual – Is referenced in the technology usage guidelines and is the detailed procedures related to technology at SFSC.

    c. Employee account creation-activation-inactivation-deletion procedure is to timely maintain appropriate employee access.

    d. Regular audits of IT security are conducted to insure that data is protected and that controls in operation are working effectively.

2. Safeguarding of physical records

    a. Maintain the student and/or job applicant information in a locked location

    b. Have procedures to only disclose information to the student or to another only upon written consent of the student/employee

3. Procedure in case of data breach

    a. In cases where access to records has been breached, the college will work to determine what information was breached and will follow FTC guidelines for contacting individuals, other businesses, and law enforcement as appropriate to instance.

    b. The college will maintain cyber risk insurance coverage to protect against major data breaches.

C. Application of the Red Flags Rule

The two provisions listed below invoke the Red Flag Rules to apply to SFSC.

1. Human Resources Department and certain academic programs with selective admissions conduct credit and/or background checks on job applicants and prospective student applicants.

2. The college becomes a creditor with covered accounts when offering institutional loans/payment arrangements to students and when offering a tuition installment plan.

D. Identifying relevant red flags to possible identity theft.

Red flags indicate patterns, practices, and specific activities that signal possible identity theft and may take the form of any of the following type of activity but they are not limited to the activities identified below:

1. Alerts, notifications, or warnings from a consumer reporting agency - Financial Aid verifies status of prospective student loan applicants with the NSLDS. If a student has a negative or conflicting history, appropriate action is taken.

2. Suspicious documents

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

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

   c. Other information on the identification is not consistent with readily accessible information that is on file with the college such as birth date or the information being presented by a new student or employee is not consistent to itself.

   d. An application for employment or admission appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

3. Suspicious personally identifying information, such as a suspicious address

   a. Human Resources Department and programs with selective admissions using fingerprint and background checks might find the external reported personally identifiable information inconsistent with what was submitted to the college.

   b. The college might receive notice that SSNs reported to the IRS have never been issued or are listed on the Social Security Administration's Death Master File. For instance, social security numbers never start with 666 or 000. As well, the numbers 987-65-4320/987-65-4329 are reserved for use in advertisements and should not be submitted.

4. Unusual use of, or suspicious activity relating to, a covered account

a. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

b. The college is notified of unauthorized charges or transactions in connection with a student's account.

c. The college is notified that checks are not arriving even after the address has been verified as others with access to the student's mailbox have taken college checks without the student's knowledge.

5. Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

a. The college might receive notice that an individual has been an identity theft victim and that certain activity on their account was not done by them. They would likely bring in court documentation, attorney's letters, police reports, etc.

b. Information from fingerprint and background checks might conflict with information already provided to the college and need clarification with official documentation to determine accuracy of represented personal information.

E. Detecting and responding appropriately to detected red flags to prevent and mitigate identity theft. SFSC employees will:

1. Verify name and/or address changes to information on file for reasonableness and will also seek to verify with appropriate government or externally issued official documentation.

2. Restrict ability of employees to change personal information to those who have been trained to spot identity theft red flags.

3. Bring changes to personal information that do not appear to be proper to the attention of a supervisor to review the situation and respond appropriately. Supervisors should work to resolve the situation but if the problem cannot be resolved within their span of control, then the college risk manager will be alerted so that the appropriate response can be coordinated. Law enforcement will be called by the risk manager if the situation warrants.

4. Verify that third party service providers have a program to identify the red flags of identity theft appropriate to the service that they provide the college and students.

F. Student identity theft awareness

1. A privacy Webpage will link from the college's homepage and summarize the college's privacy policy and procedures.

2. Awareness of identity theft will be raised through the privacy webpage linking users to the FTC website so they can identify the risks of identity theft and know what to do if they suspect they are a victim of identity theft.

The technology committee will act as the cross-functional group responsible to at least annually discuss, review and implement changes to the college's privacy and identity theft prevention program. The technology committee will report and recommend its changes to the President's Council so that privacy and identity theft prevention measures are known and made part of the control procedures in operation at the college by appropriate administrators

HISTORY: Last Reviewed: 2/17/09

Adopted: 2/17/09
Reviewed: -
Revised: -