Background

Southeastern Illinois College ("College") developed this Identity Theft Prevention Policy ("Policy") pursuant to the Federal Trade Commission's Red Flag Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with consideration of the size of the College's operations and covered accounts, the nature and scope of the College's activities. The College has implemented multiple measures and ongoing training to engage the rule.

Purpose

An Identity Theft Prevention Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a Covered Account or an existing Covered Account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

- Identify relevant Red Flags for Covered Accounts it offers or maintains and incorporate those Red Flags into the Program.
- Detect Red Flags that have been incorporated into the Program.
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
- Ensure the Program is updated periodically to reflect changes in risks to students and employees pertaining to identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions

- **Identity Theft** – Fraud committed or attempted use of identifying information of another person without authority.
- **Covered Account**- An account that a creditor offers or maintains, primarily for a person that involves or is designed to permit multiple payments or transactions.
- **Red Flag** – A pattern, practice or specific activity that indicates the possible existence of identity theft.
- **Personal Information** – Personal information is identifying information which is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person including: name, address, telephone number, social security number, date of birth, government issues driver's license or identification number, alien

registration number, government passport number, employer or taxpayer identification number, computer's Internet Protocol address, bank routing codes or accounts.

Identity Theft Prevention Program Report

The Red Flags Rule allows the College to design and implement an identity theft prevention program that is appropriate to the College's size, complexity and the nature of operation. Since the College is a creditor of student accounts subject to the Red Flags Rule, the College is required to develop and implement an identity theft prevention program.

Key Department Affected by Program

- Administration and Finance Office/ Business Affairs
- Auxiliary Services
- Student Services
    - Financial Aid
    - Registration/ Enrollment Services
    - Support Services
    - Athletics
- Human Resources
- Marketing
- Academics
- Information Technology

Existing Policies and Practices

Many offices at the College maintain records of students (along with parent information), employees (along with family information), and alumni. These records can be in paper and/or electronic form. The records are safeguarded to ensure the privacy and confidentiality of each of these individuals. The controls by the College over privileged information include:

- Students are given the opportunity to release certain information (billing, financial aid, and registration) to a third party (parents or grandparent) by signing the FERPA (Family Education Rights and Privacy Act) release form.
- Relevant employees are trained to know FERPA regulations.
- Social Security numbers are not used as primary identification numbers.
- The College is sensitive to personal data, and will not disclose any information unless by written request or a legitimate "need-to-know" basis.
- The College's official personnel files for all employees are retained in the Human Resources Office. Employees have the right to review the materials contained in their personnel file as specified by 820 ILCS 40 Personnel Record Review Act.
- The College ensures that its websites containing personally identifiable information are secure.
- The College securely destroys paper document and files containing student or employee information when a decision is made to no longer retain such information.

- The College's office computers are secured with password access.
- The College's virus protection is consistently up-to-date.
- Offices and storage rooms that contain critical information are secured at the end of each workday or when they are unsupervised.
- All student workers are required to sign a Statement of Understanding regarding confidential student records protected by the Family Educational Rights and privacy Act of 1974.
- Student workers identified as being in areas with confidential and sensitive information must agree to a criminal background check.
- The College's Acceptable Use Policy regularly goes through review and is updated for increased protection.
- Third Party Payment plan vendors are required to abide by Red Flags.
- The college has implemented an email phishing training program for employees.
- Background checks are performed during the employee hiring process where applicable.

Step 1: Identification of Relevant Red Flags

Identification of relevant red flags includes, but is not increasingly limited to, the following circumstances and examples:

- Presentation of suspicious documents and/or suspicious activities related to accounts.
    1. There is a name discrepancy on identification.
    2. Altered or falsified identification is presented.
    3. Description information on ID does not match photo or presenter of the ID.
    4. Account activity is inconsistent with prior use.
    5. Mail sent to a student is consistently returned as "undeliverable."
    6. Submission of Social Security Numbers already assigned to another individual.
- Alerts, Notifications, or Warnings from Consumer Reporting Agency
    1. A fraud or active duty alert is included with a consumer report.
    2. A consumer reporting agency provides a notice of address discrepancy.
- Unusual Use of, or Suspicious Activity Related to, the Student Account
    1. A student account is used in a manner that is not consistent with established patterns of activity on the account.
    2. A student account that has been inactive for a reasonable lengthy period of time is used.
- Notices from Students, Victims of Identity Theft, Law Enforcement Authorities or Others
- The College is notified by a student, a victim of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with student accounts held by SIC.

Step 2: Detection of Red Flags

In addition to identifying potential Red Flags, the College will also perform the following to detect when Red Flags could possible occur:

- Train staff on how to recognize, record, and report suspected red flag activity.

- Ensure all requested information to establish an account has been provided and matches other available information.
- Establish an individual or group of individuals who act as the point of contact for all red flag-related activity by monitoring and reporting the activity.
- Obtain identifying information about and verifying the identity of newly hired employees.
- Monitor transactions through photo ID (Driver's License/ the College Student ID Card) verification.
- Require an alternative identification method if photo ID appears to be altered or forged.
- Reject any application for a service or transaction that appears to be altered or forged.
- Verify the identity of individuals requesting a change in name, address, or other account information.

Step 3: Responding to Red Flags

Once red flags have been identified and detected, the College must respond to the situation according to an established plan, and notify the affected parties. Responding to red flags includes some or all of the following, which should be performed within 48 hours of detection:

- Once detected, gather all related documentation and write a description of the situation. Present this information to the Identity Theft Prevention Officer who will then determine if the transaction is fraudulent.
- Contact the owner of the covered account or the identity theft victim that is being questioned by phone, email, letter, or other source of communication.
- Cancel the transaction
- Monitor an account for evidence of identity theft.
- Notify the appropriate law enforcement if appropriate.
- Change any passwords that permit access to the covered account.
- Close existing covered account and reopen a new covered account.
- Determine that no response is warranted under the particular circumstances.

Step 4: Administering the Program

Administering the program will consist of the following duties:

- Staff training as necessary and applicable to effectively implement the program.
    1. Training may consist of several requirements of the Red Flags Rule, the policies and procedures that are set forth in this program, and the importance placed by the College on compliance with the program and the prevention and mitigation of identity theft.
    2. Training topics may include:
        A. Ensure College website is secure when user of site is providing personally identifiable information or provide clear notice that the website is not secure;
        B. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer retain such information;
        C. Ensure office computers with access to student account information are password protected;
        D. Limit use of social security numbers;

E. Keep computer virus protection up to date;
F. Require and keep only student information that is necessary for college purposes;
G. Provide Release of Student Information Guidelines to new and current staff who work with student records, financial aid or other personally identifiable information;
H. Require good passwords; and,
I. Phishing education.

- Overseeing service providers
  1. It is the responsibility of the College to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Oversight of the Program

Responsibility for developing, implementing and updating this Program lies with the Identity Theft Prevention Officer (ITPO). The ITPO will be responsible for the program administration, for ensuring the detection of Red Flags and the steps for presenting and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program. The ITPO will convene the Identity Theft Prevention Committee as needed to update the program.

Responsibilities of the committee include:
1. Investigating identity theft, fraud, and information security concerns.
2. Establishing roles and responsibilities
3. Defining confidential and sensitive information
4. Taking inventory of information assets.
5. Reviewing the Identity Theft Prevention Policy.
6. Implementing security measures.
7. Monitoring, evaluating, and enforcing the identity theft prevention program.

Updating the Program

The Program will be periodically reviewed and updated to reflect changes in risks to students and the College. As needed, the Identity Theft Prevention Officer will lead the discussion regarding the College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the College's business arrangements with other entities. If warranted, the Program will be updated.

For additional information on the Federal Trade Commission's Red Flags Rule, please visit the following website: http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml

Adopted: March 22, 2012
Amended: January 21, 2014/October 24, 2019
Legal Ref: (5ILCS 179) Identity Protection Act
Cross Ref