Orangeburg-Calhoun Technical College
Statement of Procedure

Title: Identity Theft Red Flag Program

Number: 7.006.01
Page: 1 of 4

Department of Responsibility: Vice President for Business Affairs

Authorization:

President

Date Approved: October 20, 2009

Last Revised: February 20, 2024
Last Reviewed: February 18, 2025

This procedure is established to meet the requirements of the "Red Flag Rules" regulations. These regulations require financial institutions and creditors with covered accounts to develop and implement a written identity theft prevention program in compliance with the Federal Trade Commission Red Flag Rule and related regulations of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, an amendment to the Fair Credit Reporting Act.

The purpose of the Identity Theft Program is to reduce the risk of identity theft by requiring greater attention and awareness to fraud prevention in order to protect student personal identifying information. The goal is to identify and address "Red Flags" that appear in the normal course of business operations. This document will serve as the College's "program".

The provisions require the program to be tailored to the size, complexity, and nature of the operation. The program must contain reasonable policy and procedures addressing four required components that:

A. Identify relevant Red Flags for new and existing student accounts and incorporate the Red Flags into an Identity Theft program;

B. Detect Red Flags that have been incorporated into the program;

C. Respond appropriately to identified Red Flags that are detected and mitigate identity theft; and

D. Ensure the program is updated periodically to reflect changes in risks to students

Orangeburg-Calhoun Technical College
Statement of Procedure

Part A: Identification of Relevant Red Flags

The College has identified the following as examples of "Red Flags" for students' accounts that may occur in the normal course of operations. The list is intended to be a guide to assist employees but is not all-encompassing.

1. Suspicious documents which appear to be forged, altered, etc.

2. Suspicious personal identification information that provides inconsistencies in data (different birth dates, addresses, etc.)

3. Suspicious activity on a student account

4. Notices from outside individuals or agencies.

5. Alerts, Notifications, or Failed Processing by credit or debit card companies (card refused or declined, notification to seize card, etc)

Part B: Detection of Red Flags

College personnel will take one or more of the following steps to obtain and verify the identity of the person associated with the creation and maintenance of an account, to monitor account activity, and to address account discrepancies.

1. Verify account identity with picture identification at the time of issuance or renewal of the College identification badge;

2. Require College identification badge for necessary financial transactions for current students or alternate identification for non-current students. Some transactions, depending on type, could require additional forms of identification (birth certificate, passport, driver's license, preprinted check or deposit slip, etc.);

3. Verify the identification of students if they request information using any method;

4. Verify the validity of requests to change address information and provide a reasonable means of promptly reporting incorrect address changes;

Part C: Protection, Prevention, and Mitigation of Identity Theft

College personnel will undertake one or more of the following appropriate response actions to protect student identifying information and prevent and mitigate the risk of identity theft.

1. Ensure that the College portal providing access to account information is secure;

2. Ensure that office computers with access to student and personal information are password protected;

3. Ensure that access to student and account information is appropriately authorized;

4. Ensure that access to personal information by the owner is accessible through a unique username and password;

5. Ensure College computer virus protection software is current and active;

6. Avoid the use of social security numbers for identification;

7. Require and store only information that is necessary for College purposes;

8. Ensure the complete and secure destruction of paper and electronic documents containing information about an account when it is determined that it is no longer necessary to maintain it.

9. Ensure that students' credit card information is never stored or saved electronically or on paper

10. Be alert to any suspicious activity involving credit card processing devices for tampering or substitution. Periodically inspect credit card processing devices for such tampering or substitution.

11. Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.

12. Monitor covered accounts for evidence of identity theft;

13. Notify the Vice President for Business Affairs (or designee) of any Red Flag detection for determination of actions to take;

14. Notify Law Enforcement as necessary

Part D: Program Administration, Assessment and Modification

Responsibility for administration, assessment, and monitoring of the program rests with the office of the Vice President for Business Affairs.

The Vice President for Business Affairs (or designee) will ensure appropriate employees are trained in the detection of Red Flags and the steps to be taken in the event a Red Flag is detected.

The Identity Theft Program will be reviewed annually by the Vice President for Business Affairs (or designee), as required. The College will assess the effectiveness of the policy and procedures associated with the program with respect to changes in risk to students. The assessment will include:

1. Analysis of the College's experiences with identity theft situations;

2. Consideration of changes in the identification of Red Flags;

3. Methods used to detect Red Flags;

4. Methods used to protect, prevent and mitigate identity theft; and

5. Identification of changes in agreements with service providers.

Any changes to the program as a result of the annual review will be approved by the president of the College and employees will be notified of these changes.