COLLEGE ADMINISTRATIVE PROCEDURE MANUAL

Procedure Title	Procedure Number	Page(s)	Date Adopted:
Identity Theft Prevention	CS - I	4	08/26/2025

BASED ON BOARD POLICY

Section	Policy Title	Policy Number	Date Adopted:
C - Business and Support Services	Information Security	CS	08/26/2025

PURPOSE

The purpose of this policy is to establish an Identity Theft Prevention Program 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 procedures to:

I. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program;
II. Detect red flags that have been incorporated into the Program;
III. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
IV. Ensure the Program is updated periodically to reflect changes in risks to students, faculty, and staff and to the safety and soundness of the creditor from identity theft.

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

PROCEDURE

Definitions

- Identity theft means fraud committed or attempted using the identifying information of another person without authority.
- Red flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- Covered Account means a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition and fee installment payment plan.

Covered Accounts

McLennan Community College has identified four types of accounts which are covered accounts administered by the College.

College covered accounts:

I. Student tuition and fee payment plans
II. Student ID (debit) card accounts in the bookstore
III. Payment of faculty and staff computer purchases through payroll deduction
IV. Offering institutional loans to students

Identification of Relevant Red Flags

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

I. The types of covered accounts as noted above
II. Methods provided to open covered accounts which require acceptance to the College and enrollment in classes requires the following information:
    a. Common applications with personally identifying information
    b. High school and college transcripts
    c. Official test scores
    d. Medical history
    e. Immunization history
III. The methods provided to access covered account:
        i. Disbursement obtained in person require picture identification
        ii. Disbursements obtained by mail can only be mailed to an address on file
IV. The College's previous history of identity theft.

The Program identifies the following red flags:

I. Documents where the photo ID does not resemble its owner or an application which appears to have been cut up, re-assembled and photocopied.
II. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification.
III. A request made from a non-College issued e-mail account.
IV. A request made to mail something to an address not listed on file.
V. Unusual use or suspicious account activity showing material changes in payment patterns, notification that the account holder is not receiving a mailed statement, or that the account has unauthorized charges.

VI. Notice from a victim of identity theft, law enforcement, or other persons regarding possible identity theft in connection with covered accounts.

Detection of Red Flags

Employees shall undertake reasonable diligence to identify red flags in connection with the opening of covered accounts as well as existing covered accounts through such methods as:

I. Obtaining and verifying identity
II. Authenticating customers
III. Monitoring transactions
IV. Verifying validity of address changes

Appropriate Responses to Red Flags

The detection of a red flag by an employee shall be immediately reported to the appropriate administrator and based on the type of red flag, the administrator and chief security officer will determine the appropriate response. The administrator will investigate the threat of identity theft to determine if a breach has occurred and will respond appropriately to prevent future identity theft breaches. Upon review of the incident, the responsible administrator and chief security officer shall determine what steps may be required to mitigate any issues that arise in the review. In addition, referral to law enforcement may be required. The following actions will be used in response to Red Flags;

I. Monitoring affected accounts
II. Denying access to the covered account
III. Contacting the student or affected person
IV. Changing passwords
V. Providing a new student identification number
VI. Notifying the appropriate administrator
VII. Notifying law enforcement
VIII. Determining that no response if warranted under the circumstances