Title: Identity Theft (Red Flag Rule)

Related Policy and Procedures:

Division of Responsibility: Business and Administrative Services, Institutional Research, Planning, Effectiveness and Technology

I. POLICY OVERVIEW

This Policy is intended to meet the requirements of the Federal Trade Commission (FTC) "Red Flag Rule." Identity theft is a fraud committed or attempted using the identifying information of another person without that person's authority. The College shall undertake reasonable measures to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," and to establish a system for reporting and responding to a security incident.

II. DEFINITIONS

A. **Covered Account** – A covered account is 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 or fee installment payment plan.

B. **Creditor** – A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college is a "creditor" are:

1. Offering loans to students, faculty or staff;
2. Offering a plan for payment of tuition or fees throughout the semester rather than requiring full payment at the beginning of the semester.

C. **Identifying Information** – 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 issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, routing code or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

D. **Red Flag** – A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

E. **Security Incident** – A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

III. IDENTIFICATION OF RED FLAGS

Broad categories of "Red Flags" include the following:

A. **Alerts** – alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies.

B. **Suspicious Documents** – such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.

C. **Suspicious Personal Identifying Information** – such as discrepancies in address, Social Security Number or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.

D. **Unusual Use or Suspicious Account Activity** – such as material changes in payment patterns, notification that the account holder is not receiving mailed statements, or that the account has unauthorized charges.

E. **Notice from Others Indicating Possible Identity Theft** – such as the College receiving notice from a victim of identity theft, law enforcement or another account holder reports that a fraudulent account was opened.

IV. RESPONSE AND MITIGATION

A. **Immediate Action Protocols** Upon the detection of a Red Flag, the College shall implement one or more of the following protective measures to secure the account:

1. **Verification:** Contact the account holder through a secure, secondary communication method (other than the one used for the suspicious request) to verify authenticity.
2. **Restrict Access:** Place a temporary freeze on the account or financial aid disbursement until the individual's identity is confirmed.
3. **Security Reset:** Mandate an immediate password change and enable multi-factor authentication (MFA) for the affected account.

B. **Internal Reporting and Escalation** Any employee who discovers a potential security incident or Red Flag must immediately notify their direct supervisor and the Vice President/Chief Financial Officer (CFO).
    1. **Administrative Review:** The CFO shall evaluate the incident to determine necessary mitigation steps and, where criminal activity is suspected, coordinate a referral to law enforcement.
    2. **Governance Notification:** In the event of a confirmed security breach, the President shall notify the Board of Trustees. The Board, in consultation with legal counsel, shall ensure full compliance with the notification requirements of **N.C.G.S. § 75-65**.

C. **External Breach Notification** If a security breach involving personal identifying information is confirmed, the College shall notify the affected individuals and the North Carolina Attorney General's Office in the timeframe and manner prescribed by **N.C.G.S. § 75-65**.

V. TRAINING

To ensure continued effectiveness and compliance with FTC regulations:

A. **Annual Training:** All College employees who process or manage information related to a "covered account" must complete identity theft prevention training annually.
B. **Policy Audit:** This policy and the associated Identity Theft Prevention Program shall be reviewed and updated annually by the Identity Theft Compliance Officer to reflect changes in identity theft risks and technological advancements.

Legal Reference: Fair and Accurate Credit Transactions Act (FACTA) of 2003;16 CFR § 681 (FTC Regulations – Red Flag Rule); N.C.G.S. § 75-65; N.C.G.S. § 132-1.10.

June 13, 2023	June 9, 2026	June 9, 2026
Date Approved by Board of Trustees	**Date of Last Review**	**Date of Last Revision**