I. POLICY OVERVIEW

This Policy is intended to meet the requirements of the 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 a security incident.

II. DEFINITIONS

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.

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 or college is a "creditor" are:

1. Participation in the Federal Perkins Loan program;
2. Participation as a school lender in the Federal Family Education Loan Program;
3. Offering loans to students, faculty or staff;
4. Offering a plan for payment of tuition or fees throughout the semester rather than requiring full payment at the beginning of the semester.

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.

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

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:

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

2. Suspicious Documents - Documents 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, or similarly altered documents.

3. Suspicious Personal Identifying Information - 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; failure to provide all required information; or other similarly suspicious information.

4. Unusual Use or Suspicious Account Activity - Material changes in payment patterns, notification that the account holder is not receiving mailed statements or that the account has unauthorized charges, or other similar activity.

5. Notice from Others Indicating Possible Identity Theft - Notices from a victim of identity theft, law enforcement or another account holder reports that a fraudulent account was opened, or other similar notices.

IV. DETECTION OF RED FLAGS

College 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:

1. Obtaining and verifying identity;
2. Authenticating customers; and
3. Monitoring transactions.

A data security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone

fraudulently claiming to represent the College or to a fraudulent web site may heighten the risk of identity theft and should be considered Red Flags.

V. SECURITY INCIDENT REPORTING

College employees who believe that a security incident has occurred shall immediately notify their appropriate supervisor, the divisional Executive Leader, and the Chief Financial Officer. Upon review of the incident, the Chief Financial 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.

If there is a security breach, the College shall comply with all notice requirements contained in N.C.G.S. § 75-65.

VI. TRAINING

All College employees who process any information related to a covered account shall receive annual training and this Policy shall be reviewed annually.

REFERENCES

Statutory References	N.C.G.S. § 75-65, Fair and Accurate Credit Transactions Act of 2003
Regulatory References	FTC Regulations - Red Flag Rule
Relevant Guidance	"N.C. Community College Written Memoranda CC10-029" (2003)
Policy Manual Cross-References	None

POLICY HISTORY

November 12, 2025	Adopted.