II. F. Identity Theft Prevention

Effective Date: May 3, 2012

Revises Previous Effective Date: N/A, New Policy

I. POLICY:

This Identity Theft Prevention Policy is adopted in compliance with the Federal Trade Commission's "Red Flags Rule", which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The purpose of this policy is to establish an Identity Theft Prevention Program 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 administration of the Identity Theft Prevention Program.

II. APPLICABILITY:

All work units and technical colleges associated with the Technical College System of Georgia.

III. DEFINITIONS:

Identity Theft - fraud committed or attempted using the Identifying Information of another person without authority.

Red Flag - a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Covered Account - a consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly, or multiple payments in arrears, in which a "continuing relationship" is established. This includes an account a College offers or maintains, primarily for personal, family or household purposes, that involves or is designated to permit multiple payments or transactions, such as a credit card account, student account or other financial account. This also includes any account that the College maintains for which there is a reasonably foreseeable risk to customers from Identity Theft.

Program Administrator - the individual designated with primary responsibility for oversight of the program. See Section V (D) below.

Identifying Information or **Personal 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, government issued identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

Identity Theft - fraud committed using the personal Identifying Information of another person.

IV. ATTACHMENTS:

None.

V. PROCEDURE:

A. IDENTIFICATION OF RED FLAGS—In order to identify relevant Red Flags, each College must consider the types of accounts that it offers and maintains, methods it provides to open accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The following Red Flags must be considered by each College:

1. **Notifications and Warnings from Credit Reporting Agencies—Red Flag**
    a. Report of fraud accompanying a credit report;
    b. Notice or report from a credit agency of a credit freeze on an applicant;
    c. Notice or report from a credit agency of an active duty alert for an applicant;
    d. Receipt of a notice of address discrepancy in response to a credit report request; and
    e. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

2. Suspicious Documents—Red Flags:

a. Identification document or card that appears to be forged, altered or inauthentic;
b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
c. Other document with information that is not consistent with existing student information; and
d. Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information—Red Flags:

a. Identifying Information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
b. Identifying Information presented that is inconsistent with other sources

of information (for instance, an address not matching an address on a loan application);
c. Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;
d. Identifying Information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
e. Social security number presented that is the same as one given by another student;
f. An address or phone number presented that is the same as that of another person;
g. A person fails to provide complete personal Identifying Information on an application when reminded to do so; and
h. A person's Identifying Information is not consistent with the information that is on file for the student.

4. Suspicious Covered Account Activity or Unusual Use of Covered Account —Red Flags:

1. Change of address for a Covered Account followed by a request to change the student's name;
2. Payments stop on an otherwise consistently up-to-date Covered Account;
3. Covered Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the College that a student is not receiving mail sent by the College;
6. Notice to the College that a Covered Account has unauthorized activity;
7. Breach in the College's computer system security; and
8. Unauthorized access to or use of student Covered Account information.

5. Alerts from Others—Red Flag:

Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

In addition, each College shall consider whether or not additional Red Flags should be identified after considering the College's Covered Accounts, methods of providing Covered Accounts, methods of accessing Covered Accounts and previous experience with Identity Theft. The need to add additional Red Flags shall be reviewed annually by the College's Vice President of Administration. To the extent the College adds additional Red Flags, these shall written and distributed to appropriate College personnel on at least an annual basis. A copy shall be maintained in the custody of the College's Vice President of Administration.

B. DETECTING RED FLAGS

1. Student Enrollment—In order to detect any of the Red Flags identified above associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening the Covered Account:
    a. Require certain Identifying Information such as name, date of birth, academic records, home address or other identification; and
    b. Verify the student's identity at time of issuance of student identification card by review of driver's license or other government-issued photo identification.

2. Existing Covered Accounts—In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take the following steps to monitor transactions on an account:
    a. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
    b. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
    c. Verify changes in banking information given for billing and payment purposes.

3. Consumer ("Credit") Report Requests—In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, College personnel will take the following steps to assist in identifying address discrepancies:
    a. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
    b. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the College has reasonably confirmed is accurate.

C. PREVENTING AND MITIGATING IDENTITY THEFT—In the event College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag, type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and other factors:

1. Prevent and Mitigate

a. Continue to monitor a Covered Account for ongoing evidence of Identity Theft;
b. Contact the student or applicant (for which a credit report was run);
c. Cancel the transaction;
d. Change any passwords or other security devices that permit access to Covered Accounts;
e. Not open a new Covered Account;
f. Provide the student with a new student identification number and/or account number;
g. Notify the Program Administrator for determination of the appropriate step(s) to take;
h. Notify law enforcement when applicable;
i. Determine that no response is warranted under the particular circumstances.

2. Protect Student Identifying Information—In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student Identifying Information:
   a. Ensure that its website is secure 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 maintain such information;
   c. Ensure that office computers with access to Covered Account information are password protected;
   d. Avoid use of social security numbers (See College Information Use Policy);
   e. Ensure computer virus protection is up to date; and
   f. Require and keep only the kinds of student information that are necessary for College purposes.

D. PROGRAM ADMINISTRATION

1. Oversight—Each College's Vice President for Administration ("VPA") is responsible for the oversight of the Program and is the "Program Administrator" for that College. The VPA and the College's Vice President of Student Services are responsible for the development, implementation, administration, and the annual review of the Program.

2. Staff Training and Reports—The College will implement annual training to emphasize the importance of meaningful data security practices and to create a "culture of security." The College acknowledges that a well-trained workforce is the best defense against Identity Theft and data breaches.
   a. Annually explain the Program rules to relevant staff, and train them to spot security vulnerabilities, and update them about the new risks and

vulnerabilities.

b. Have relevant staff signs a statement acknowledging that they read and understand the Program.
c. Advise employees that violation of this policy is grounds for discipline, up to, and including dismissal.

3. Service Provider Arrangements—The College will, as part of its contracts with third party service providers, require as a part of the contract that these providers have policies, procedures and programs that comply with the "Red Flag" rule, that the provider is aware of this policy, and that the provider will report to the College any Red Flags it identifies as soon as possible

4. Program Updates—the College's VPA will review the program annually and make recommendations for substantial changes to the program, if necessary. Any known Identity Theft incidents and the response to the incident will be reported immediately to the College President and the TCSG Assistant Commissioner, Administration (or equivalent position)..

VI. RECORD RETENTION

Not Applicable.