POLICY TITLE: IDENTITY THEFT PROTECTION POLICY

I.   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 policies and procedures to:

1.   Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;

2.   Detect red flags that have been incorporated into the Program;

3.   Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

4.   Ensure the Program is updated periodically to reflect changes in risks to Students 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.

II.   Definitions

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

Covered account means all student accounts or loans that are administered by the College.

A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Identifying information means any name or number that may be used, alone or in conjunction with any other information, to identity 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, or bank routing code.

III. Policy/Procedure

A. Red Flag Detection Procedures
In order to detect any of the Red Flags associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening an account:

1. Require identifying information such as name, date of birth, academic records, home address or other identification
2. Verify the student's identity at the time of issuance of a student identification card (review of valid driver's license or other government-issued photo identification).

B. Covered Accounts
Lansing Community College has identified five types of accounts, four of which are covered accounts administered by the College and one type of account that is administered by a service provider.

College covered accounts:

1. Refund of credit balances involving Federal PLUS loans
2. Refund of credit balances involving Federal Stafford loans
3. Refund of credit balances involving Alternate (Private) loans
4. Deferment of tuition payments

Service provider covered account:

1. Tuition payment plan administered by FACTS, refer to "Oversight of Service Provider Arrangements".

C. Identification of Relevant Red Flags
The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above;
2. The methods provided to open covered accounts
   Acceptance to the College and enrollment in classes requires the following information:
   - Common application with personally identifying information high school transcript
   - Online Free Application for Federal Student Aid (FAFSA) or Private Lender application

3. The methods provided to access covered accounts:
   Disbursement obtained in person require picture identification
   Disbursements obtained by mail can only be mailed to an address on file

4. The College's previous history of identity theft.

The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged;

2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;

3. Inconsistent information from credit checks or enrollment status including recent address changes.

4. A request made from a non-College issued E-mail account;

5. A request to mail something to an address not listed on file; and

6. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

D. Detection of Red Flags
The Program will detect red flags relevant to each type of covered account as follows. Specifics of detection methods and processes will be shared with individuals involved in those processes.

1. **Refund of a credit balance involving a PLUS loan** – As directed by federal regulation (U.S. Department of Education) these balance are required to be refunded in the parent's name and mailed to their address on file within the time period specified. No request is required. **Red Flag** –Parent refund address change with signature or notary seal not appearing authentic. Multiple refunds with the same or similar contact attributes (address, phone, etc.).

2. **Refund of credit balance, non PLUS loan** – requests from current students must be made in person by presenting a picture ID or in writing from the student's college issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing picture ID. Requests from students not currently enrolled or graduated from the college must be made in writing. **Red Flag** – Picture ID not appearing to be authentic or not matching the

appearance of the student presenting it. Request not coming from a student issued e-mail account. Multiple refunds with the same or similar contact attributes (address, phone, etc.).

3. **Deferment of tuition payment** – requests are made in person only and require the student's signature. **Red Flag** – none.

4. **Tuition payment plan** – Students must contact an outside service provider and provide personally identifying information to them. Red Flag – none, see Oversight of Service Provider Arrangements.

E. Response
The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;

2. Contact the student;

3. Change any passwords, security codes or other security devices that permit access to a covered account;

4. Notify law enforcement and/or Department of Education for Federal Loans; or

5. Determine no response is warranted under the particular circumstances.

IV.   Responsibility

A. Oversight of the Program
Responsibility for developing, implementing and updating this Program lies with the Executive Vice President for Operations. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of College's staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Updating the Program
This Program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the College from identity theft. At least once per year, the Program Administrator will consider the

College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted.

C. Staff Training

College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

D. Oversight of Service Provider Arrangements

The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. Currently the College uses FACTS to administer the Tuition Payment Plan. Students contact FACTS directly through its website and provide personally identifying information to be matched to the records that the College has provided to FACTS.

Adopted: April 20, 2009