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 employees or to the safety and soundness of students and employees from Identity Theft.

Covered Accounts

The University has identified the following types of accounts, which are covered accounts administered by the University or are administered by a service provider:

University Covered Accounts

1. Refund of credit balances involving Student Loans

2. Refund of credit balances without Student Loans

3. Deferment of Tuition Payments

4. Emergency Loans

5. Millersville Installment Payment Plan

6. Marauder Card Accounts

Accounts Covered by a Service Provider

1. Perkins Loan

Identification of Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The University identifies the following Red Flags in each of the listed categories:

Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;

2. Notice or report from a credit agency of a credit freeze on an applicant;

3. Notice or report from a credit agency of an active duty alert for an applicant;

4. Receipt of a notice of address discrepancy in response to a credit report request; and

5.
pattern or activity.

Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;

2. description is not consistent with the person presenting the document;

3. Other document with information that is not consistent with existing student information; and

4. Application for service that appears to have been altered or forged.

Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);

2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);

3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

   a. Social Security number presented that is the same as one given by another student;

   b. An address or phone number presented that is the same as that of another person;

   c. A person fails to provide complete personal identifying information on an application when reminded to do so; and

   d. file for the student.

Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an name;

2. Payments stop on an otherwise consistently up-to-date account;

3. 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 University that a student is not receiving mail sent by the University;

6. Require and keep only the kinds of student information that are necessary for University purposes.

Program Administration

Oversight

Responsibility for developing, implementing and updating this Program lies with the Identity Theft Committee
the Associate Vice President of Finance and Administration as appointed by the President. The remainder of the Committee is comprised of the Registrar, the Director of Financial Aid, the Bursar, the Director of Administrative Information Services and the Director of Compensation and Benefits and others as deemed necessary. The Committee will be responsible for ensuring appropriate training of the University 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.

Staff Training and Reports

University staff responsible for implementing the Program shall be trained either by or under the direction of the Committee in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Committee once they become aware of an incident of Identity Theft or of the At least annually or as otherwise requested by the Committee, University staff responsible for development,

Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices

not be shared with other University employees or the public. The Committee shall inform those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the University from Identity Theft. In doing so, the
tity Theft situations,
changes in Identity Theft methods changes in Identity Theft detection and prevention

After considering these factors, the Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.