Identity Theft Prevention Program

I. Title of Policy
Identity Theft Prevention Program (the "Program")

II. Objective of Policy
To establish the Program designed to reasonably 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.

III. Authority
Federal Trade Commission final rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (the "Red Flags Rule").

IV. Policy Statement
The College has designed a Program to reasonably 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 will:

1. Identify relevant Red Flags for new and existing covered accounts that the College 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.

The Program shall, as appropriate, supplement College policies and regulations that control reasonably foreseeable risks.

Program Administration
Successful implementation of the Identity Theft Program ultimately is the responsibility of each office, the employees of each office that maintains accounts or databases covered by this Program, and the College community as a whole.

As permitted by the Red Flags Rule regulations responsibility for overseeing the Program has been delegated to the Vice President for Business and Finance, with program administration and compliance monitoring responsibility to be performed by the Director of Budget and Compliance ("Program Administrator"). The Program Administrator is responsible for:

1. The administration of the Program;
2. Ensuring the appropriate Program training for the College's staff;
3. Reviewing and investigating any staff reports regarding the detection of Red Flags and compliance;
4. Ensuring the College's responsiveness to alleged incidents of identity theft;
5. Determining which steps of prevention and mitigation should be taken in particular circumstances;

6. Recommending to the Vice President for Business & Finance material changes to this policy, as necessary to address changing risks of identity theft; and
7. Reviewing all requests by the College's staff seeking access to student or employee social security numbers.

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

"Covered account" means an account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. These accounts include all student accounts or loans that are administered by the College.

For the purpose of the College's Identity Theft Program, the term "covered account" is extended to include any College account or database (financially based or otherwise) for which the College believes there is a reasonably foreseeable risk to the College, its students, faculty, staff, constituents, or customers from identity theft.

"Red Flag(s)" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

"Program Administrator" is the College's Director of Budget and Compliance, who has been designated with the primary responsibility for oversight of the Program.

"Identifying information" means any name or number that may be used in conjunction with any other information to identify a specific person including: name, address, telephone number, social security number, date of birth, driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number, student identification number, internet protocol address or routing code.

"Service Provider" is a person or business entity that provides a service directly to the college.

Covered Accounts
The College has identified several types of covered accounts, including accounts administered by the College and accounts administered by service providers.

1. The covered accounts administered by the College are student accounts, employee accounts, and employee records.

2. The covered accounts administered by service providers are payment plan accounts, collection accounts, and various covered accounts.

Identification of Relevant Red Flags
The following items or situations may demonstrate the existence of a Red Flag:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. The presentation of suspicious or inconsistent documents or personal identifying information;
3. The unusual use of, or other suspicious activity related to, a covered account;
4. A request made from a non-college issued e-mail account;
5. A request to mail something to an address not listed on the requestor's file;
6. Notice from a student, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Detection of Red Flags
Red Flags in connection with the opening of covered accounts and existing covered accounts shall be detected by:

1. Obtaining identifying information such as name, date of birth, home address or other identification, and verifying the identity of a person opening a covered account; and
2. Authenticating the identification of students if they request information either in person, via telephone or e-mail. Verifying the validity of change of billing address requests and in banking information for billing and payment purposes in the case of existing covered accounts.

In order to detect any of the Red Flags identified above in situations involving an employment position for which a background or credit report is sought, the College will require written verification from any applicant that the address provided by the applicant is accurate. In the event that notice of an address discrepancy is received, the College shall verify that the background and/or credit report pertains to the applicant for whom the requested report was made and report to the reporting agency an address for the applicant that the College has reasonably confirmed is accurate.

Response to Detection
The following are appropriate responses to detected Red Flags in order to prevent and mitigate identity theft:

1. Deny access to the covered account until other information is available to eliminate the Red Flags, or close the existing covered account;
2. Contact the student and/or provide the student with a new student identification number;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Re-open a covered account with a new account number or depending on the circumstances, not open a new covered account;
5. Notify the Program Administrator for a determination of the appropriate step(s) to take;
6. Notify appropriate law enforcement; or
7. Determine no response is warranted under the particular circumstances.

Reports of Identity Theft
Upon the discovery of an incident of identity theft, the manager/director of the office for which the discovery was made shall complete an identity theft detection form which shall be submitted to the Program Administrator for his or her review.

Protecting Identifying Information
The Program Administrator shall undertake the following measures with respect to the College's internal operating procedures to protect identifying information:

1. Ensure complete and secure destruction of paper documents containing identifying information when such documents or files are no longer needed;
2. Avoid use of social security numbers and allow access to social security numbers to a very limited number of staff who have been approved by the Program Administrator; and
3. Require and keep only information that is necessary for College purposes.

The Vice President of Institutional Effectiveness/CIO shall undertake the following measures with respect to the College's internal operating procedures to protect identifying information:

1. Ensure the College's website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of computer files containing identification information when such documents or files are no longer needed;
3. Ensure that office computers with access to covered account information are password protected;
4. Ensure computer virus protection is up to date; and
5. Require and keep only information that is necessary for College purposes.

Staff Training
College employees responsible for covered accounts shall be trained either by or under the direction of the Program Administrator on the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

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 regulations designed to detect, prevent and mitigate the risk of identity theft whenever the College engages a service provider to perform an activity in connection with one or more covered accounts.

Updating the Program
The Program Administrator shall review and make recommendations for updating or modifying the program to reflect changes in risks to members of the College community and the safety and soundness of the College from identity theft based on factors such as:

1. The experiences of the College with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the types of accounts that the College offers or maintains; and
5. Changes in the College's business arrangements with other entities.

November 17, 2010
Revised July 20, 2016
Revised June 19, 2018

The Program Administrator shall address material matters related to the Program and evaluate issues such as:

1. The effectiveness of the Program in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
2. Service provider agreements in light of the Program requirements;
3. Significant incidents involving identity theft and management's response; and
4. Recommendations for material changes to the Program, as necessary.

Reporting

All instances of identity theft will be reported to the Committee on Audit of the Board of Trustees. The Program Administrator will prepare a report which describes the state of the Program during the past year and recommendations for improvements to the Program. The report will be provided to the Vice President for Business & Finance.

November 17, 2010
Revised July 20, 2016
Revised June 19, 2018