Title: IDENTITY THEFT PREVENTION PROGRAM

- Initial Action: 5-27-2010
- Board Resolution:
- Last Revised:
  - Policy: 5-27-2010
  - Procedure: 5-27-2010
  - Last Reviewed:
- Effective: 6-1-2010
- Next Review: June 2011
- Responsibility: **Financial Services/Administrative Services Division**

POLICY

An Identity Theft Prevention Program is intended to detect, prevent and mitigate identity theft in connection with personal identifying information (student, donor, patron, faculty and staff) and to provide the framework for administrative oversight by an internal Committee.

I. BACKGROUND

The Financial Institution Regulators, including the Federal Trade Commission have issued a final rule (the Red Flags Rule) under sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. The Red Flags Rule requires institutions or "creditors" (businesses or organizations that regularly defer payment for goods or services) that hold "covered accounts" (i.e. consumer accounts, students accounts for which a person makes repeat payments or other accounts, i.e. employees, that present a reasonably foreseeable risk of identity theft) to develop and implement an identity theft prevention program.

Cecil College takes the possibility of identity theft seriously and in its effort to comply with the Red Flags Rule, has developed this policy and accompanying procedures based on current College operations and activities. The Board of Trustees determined that this Policy was appropriate for Cecil College, and therefore approved this policy at their May 27, 2010 board meeting with an effective date of June 1, 2010.

II. PROCEDURES

An Identity Theft Prevention Committee will oversee the implementation and training activities related to the policy, procedures and the internal business practices used to detect, prevent and mitigate identity theft.

A. The procedures shall:

1. Explain the necessity of the Identity Theft Prevention Program
2. List the Departments responsible for securing personal identifying information.
3. Define the Identity Theft Prevention Committee responsibilities and reporting structure.
4. Ensure that the policy, procedures and business practices are updated annually to reflect changes in identity theft risks.
5. Reinforce the College's responsibility to ensure that contracted service providers have identity theft prevention policies and/or procedures.

B. The internal business practices shall:

1. Identify relevant red flags for personal indentifying information
2. Establish methods to detect red flags; and
3. Define the College's response to any red flags that are detected.

III. DEPARTMENT RESPONSIBLITIES

A. Departments or Functions

The following College departments or functions are currently identified with potential exposure to identity theft, and as a result are required to maintain personal information records and data in a secure manner to prevent identity theft.

1. Academic Programs Division
2. Account Receivable: Student Accounts
3. Accounts Payable
4. Admissions and Advising
5. Cecil College Foundation
6. Family Education Center
7. Financial Aid
8. Human Resources and Payroll
9. Information Technology
10. Library
11. Mail and Duplication Services
12. Milburn Stone Theatre
13. Registration
14. Security

B. Incident Reporting

1. In the event College personnel detect a Red Flag or become aware of an incident of identity theft incident or the College' failure to comply with this policy, such personnel should communicate their findings to the Vice President of their Division or Security if immediate assistance is needed.
2. An Incident Report must also be forwarded to the Identity Theft Prevention Committee.

3. Incidents may be referred by the Program Administrator to a task force comprised of members of the Identity Theft Prevention Committee.

C. Annual Reporting and Operation Audits

1. Department staff responsible for securing personal identifying information shall provide a written report annually to the Committee.
2. The report should address material matters related to the Identify Theft Program such as the effectiveness of the policy and procedures, significant incidents involving identity theft, follow up measures or actions taken and recommendations for changes to the Program.
3. Departments are subject to periodic audits without notice of various business practices related to securing personal identifying information.

IV. PROGRAM ADMINISTRATION

A. Committee Responsibilities and Structure

1. Responsibility for developing, implementing, and updating this program (policy, procedures and business practices) lies with the College's Identity Theft Prevention Committee.
2. The Committee shall be headed by a Program Administrator and include the following College positions:

   Controller
   Director of Academic Program Support
   Director of Security
   Director of Information Technology
   Director of Records and Registration
   Human Resource Manager

3. The Program Administrator may establish a task force in order to take prompt action when an occurrence arises.
4. The Program Administrator will report directly to the Vice President of Administrative Services.
5. At a minimum, quarterly meetings should be scheduled with the full committee.
6. The Identity Theft Prevention Committee is responsible for providing training to detect red flags and steps to take when a red flag is detected to College staff responsible

B. Annual Review of Policy/Procedures

1. The Committee will update the policy and procedures to reflect changes in identify theft risks and the security of personal indentifying information within the College operations including emerging threats and prevention methods.

2. The Committee will address any program weaknesses and develop recommendations for improvement.
3. The Committee will review proposed changes with the Divisions Vice Presidents before taking revisions to the College Management Team and the President.
4. Changes to the policy require the approval of the Board of Trustees.
5. The Identity Theft Prevention Committee may also recommend changes to internal business practices and department operations on a periodic basis.

C. Service Provider Contracts or Agreements

1. The Committee will require defined service providers/vendors (i.e. Barnes & Noble, CashNet, Donate Now, Heartland, Jenzabar, etc) to have appropriate identify theft policies and procedures in place; and require them to report any red flags to the Program Administrator or the College employee with primary oversight of the service provider/vendor relationship.
2. The Committee will distribute the College's Policy annually to defined service providers at the beginning of each fiscal year.

D. Disclosure of Specific Practices

1. For the effectiveness of the Identity Theft Prevention Policy, the Red Flags Rule call for a degree of confidentiality regarding the College's specific business practices relating to Identity Theft detection, prevention and mitigation.
2. Knowledge of such specific business practices will be limited to the Identity Theft Prevention Committee and those employees who need to know them for purposes of preventing identity theft.

E. Related College Policies/Regulations

Academic Honesty Policy
Confidentiality of Library Records (October 29, 2009)
Family Education Rights & Privacy Act (FERPA)
Performance Management for College Employees (May 5, 2007)
Student Code of Conduct (August 28, 2008)
Use of Information Technology (August 1, 2004)

V. GLOSSARY OF TERMS

Identity theft is a fraud committed or attempted using the identifying information of another person without authority.

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

“Covered Account” includes personal information of students, donors, patrons and employees including all student financial aid and loan accounts that are administered by the College, any account that involves or is designed to permit multiple payments or transactions. Credit card payment information also presents an opportunity for identity theft and fraud.

Identity Theft Prevention Committee is the primary group established to carry out the identity theft procedures.

Program Administrator is the individual designated with primary responsibility for oversight of the policy and implementation of the procedures through the Committee.

Creditor means a business or organization that regularly defers payment for goods or services, or provides goods or services and bills the customer later. In this case, the College is a creditor.

Identifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, maiden 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, credit card information, or computer internet protocol (IP) address. It does NOT include transcripts or academic credentials of students or candidates for faculty or staff positions.