**IDENTITY THEFT PREVENTION (Red Flag) POLICY**

The risk to the College, its employees and students from data loss and identity theft is of significant concern to the College and can be reduced only through the combined efforts of every employee and vendor.

The College developed and adopted this Identity Theft Prevention policy pursuant to the Federal Trade Commission’s (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This program is to help protect employees and students from damages related to the loss or misuse of sensitive information.

This policy enables the College to protect existing employees and students, reducing risk from identity fraud, and minimizes potential damage to the College from fraudulent new accounts. The program will help the College identify risks that signify potentially fraudulent activity within new or existing covered accounts; detect risks when they occur in covered accounts; respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

This policy and protection program applies to employees and students at the College, including all personnel affiliated with third parties.

**DEFINITIONS AND PROGRAM**

**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 –** includes all student accounts or loans that are administered by the College. Also any business, personal and student financial aid account for which there is a reasonably foreseeable risk to the safety of the College from identity theft, including financial, operational, compliance and litigation issues.

**Sensitive or Identifying Information -** any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. It includes the following items whether stored in electronic or printed format:

1. Credit card information, including any of the following:

* Credit card number (in part or whole)
* Credit card expiration date
* Cardholder name
* Cardholder address

2.Tax identification numbers, including:

* Social Security number
* Business identification number
* Employer identification numbers

3. Payroll information, including, among other information:

* Paychecks
* Pay stubs
* Direct deposit requests

4. Flex Spending plan check requests and associated paperwork

5. Medical insurance information for any employee or student, including but not limited to:

* Doctor names and claims
* Insurance claims
* Any related personal medical information

6. Maroon Card

* Funds on the account

7. Other personal information belonging to any employee or student, examples of which include:

* Date of birth
* Address
* Phone numbers
* Maiden name
* Names
* Government issued driver’s license or I.D. number
* Alien registration number
* Government passport number
* Employee or Student Identification number
* Computer’s Internet Protocol address or routing code

**NOTE: College personnel are encouraged to use common sense in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.**

**Hard Copy Distribution -** Each employee and vendor performing work for the College will comply with the following policies:

* File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked or in a locked room when not in use or when unsupervised.
* Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.
* Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use or when unattended.
* Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
* When documents containing sensitive information are discarded they will be placed inside a locked shred bin/area or immediately shredded.

**Electronic Distribution -** Each employee and vendor performing work for the College will comply with the following policies:

* Internally, sensitive information may be transmitted using the Colleges e-mail system. All sensitive information must be secured via password protection when stored in an electronic format.
* Any sensitive information sent externally must be password protected and only to approved recipients. Additionally, a statement such as the following should be included in the e-mail: *“This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited.”*
* No sensitive information should leave the College which is not secured.

**Third Party Software or Service providers –** Each third party vendor with whom the College contracts will be required to sign a formal agreement stating that all federal laws, internal policies and safe guards by which the College must abide will be followed to insure that College data will be protected.

**IDENTIFICATION OF RED FLAGS**

In order to identify relevant Red Flags, the College 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 experience with Identity Theft. The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

**Notifications and Warnings from Credit Reporting Agencies –**

* Report of fraud accompanying a credit report;
* Notice or report from a credit agency of a credit freeze on an applicant;
* Notice or report from a credit agency of an active duty alert for an applicant;
* Receipt of a notice of address discrepancy in response to a credit report request; and
* Indication from a credit report of activity that is inconsistent with an applicant’s usual pattern or activity.

**Suspicious documents -**

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

**Suspicious personal identifying information -**

* Identify information presented that is inconsistent with other information provided (example: inconsistent birth dates);
* Identifying information presented that is inconsistent with other sources of information (for instance, an address does not match any address on file with the College);
* Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
* Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
* Social security number presented that is the same as one given by another person;
* An address or phone number presented that is the same as that of another person;
* A person fails to provide complete personal identifying information on an application when reminded to do so; and
* A person’s identifying information is not consistent with the information that is on file.

**Unusual use of, or suspicious activity related to, the covered account**

* Change of address for an account followed by a request to change the student’s name;
* Payments stop on an otherwise consistently up-to-date account;
* Account is used in a manner that is not consistent with prior use;
* Mail sent to the person is repeatedly returned as undeliverable;
* Notice to the College that mail sent by the College is not being received;
* Notice to the College that an account has unauthorized activity;
* Breach in the College’s computer system security involving personal information; and
* Unauthorized access to or use of account information.

**DETECTING RED FLAGS**

**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 account:

* Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
* Verify the student’s identity at time of issuance of student identification card (review of driver’s license or other government-issued photo identification).

**Existing 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:

* Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
* 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
* Verify changes in banking information given for billing and payment purposes.

**Employee Information –** In order to detect any of the Red Flags identified above for employees, College personnel will take the following steps to protect employee information:

* Verify the identification of employees if they request personal information (in person, via telephone, via facsimile, via email);
* Verify the validity of requests to change addresses or phone numbers by phone or email.
* Verify outside requests for verification of employee confidential information (employment verifications).

**RESPONDING TO RED FLAGS**

**Once a potentially fraudulent activity is detected, the College must act as quickly as appropriate to protect students, employees and the College from damages and loss.** All related documentation should be gathered and a description of the situation should be written. This information should be presented to a designated authority for determination. The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

**If a transaction is determined to be fraudulent, appropriate actions must be taken immediately.** Actions may include canceling the transaction; notifying and cooperating with appropriate law enforcement; determining the extent of liability of the College or damage to the College; notifying the appropriate person that a fraud has been attempted and notifying any appropriate insurers.

**In cases where an individual’s personal information on college owned systems has been compromised, the College will provide monitoring services to identify activities that could be indicators of additional fraud. This service will be offered to the individual up to one year following the original fraudulent activity.**

**PROTECTING AGAINST IDENTITY THEFT**

**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:

* Ensure that its website is secure or provide clear notice that the website is not secure;
* 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;
* Ensure that office computers with access to Covered Account information are password protected;
* Avoid use of social security numbers;
* Ensure computer virus protection is up to date; and
* Require and keep only the kinds of student information that are necessary for College purposes.

**Employee Identifying Information –** In order to further prevent the likelihood of Identity Theft occurring with respect to employees, the College will take the following steps with respect to its internal operating procedures to protect employee identifying information:

* Ensure that the employee website is secure or provide clear notice that the website is not secure;
* Ensure complete and secure destruction of paper documents and computer files containing employee information when a decision has been made to no longer maintain such information;
* Ensure that office computers with access to employee information are password protected;
* Avoid when possible the use of social security numbers;
* Ensure computer virus protection is up to date.

**PERIODIC UPDATES**

At periodic intervals, the program will be re-evaluated to determine whether all aspects are up to date and applicable in the current business environment. Periodic reviews will include an assessment of which accounts are covered by the program. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the College and its population.

**PROGRAM ADMINISTRATION**

**Involvement of management** - The Identity Theft Policy shall not be operated as an extension to any other existing fraud prevention programs. It shall be a separate stand alone policy. The Identity Theft Policy is the responsibility of the management of the College. Approval of the initial policy must be appropriately documented and approved by Cabinet. Operational responsibility of the policy is delegated to the Chief Information Officer.

**Staff training** - Staff training shall be conducted for all employees and vendors for whom it is reasonably foreseeable may come into contact with covered accounts or personally identifiable information. The CIO is responsible for ensuring identity theft training for all requisite employees and vendors. Employees must receive annual training in all segments of this policy. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

**Oversight of Vendor/Service Provider arrangements** - It is the responsibility of the College to ensure that the activities of all vendors are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A vendor that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements. Any specific requirements should be specifically addressed in the appropriate contract arrangements.