148.00 IDENTITY THEFT PREVENTION

The risk to the college, its employees and students from data loss and identity theft is of significant concern to the college and can only be reduced through the combined efforts of every employee and contractor. The college adopts this sensitive information policy to help protect employees, students, contractors and the college from damages related to the loss or misuse of sensitive information.
This policy and protection program applies to employees, contractors, consultants, temporary workers, and other workers at the college (volunteers, student ambassadors), including all personnel affiliated with third parties.

DEFINITION OF SENSITIVE INFORMATION
Sensitive information includes the following items whether stored in electronic, printed format or verbally shared:

- Personal Information – Sensitive information consists of personal information including, but not limited to:
  - Credit Card Information, including any of the following:
    - Credit Card Number (in part or whole)
    - Credit Card Expiration Date
    - Cardholder Name
    - Cardholder Address
  - Customer Payment Information, including any of the following:
    - Bank account numbers
    - Signatures required
    - EFT – EDI – Draft – Bank Information
    - Owners Name & Address
    - Insufficient check information
  - Tax Identification Numbers, including:
    - Social Security Number
    - Social Insurance Number
    - Business Identification Number
    - Employer Identification Numbers
  - Tax Related Information, including:
    - W-2's & W-4's
    - 1099's & 1098's
    - Specific Tax Related Information Related to Filing
    - Tax Related Information for any employees or students
  - Payroll Information, including, among other information:
    - Paychecks
    - Pay stubs
    - Timecard information
  - Cafeteria Plan Check Requests and associated paperwork (including online information)
  - Medical Information for any employee or student, including but not limited to:
    - Doctor names and claims
    - Insurance claims
    - Prescriptions
    - Any related personal medical information
  - Other Personal Information belonging to students, employees and contractors, examples of which include:
    - Date of Birth
    - Address
    - Phone Numbers
    - Maiden Name
    - Names

    - Student Number
- College Information – Sensitive college information includes, but is not limited to:
    - College, employee, student, vendor, supplier confidential, proprietary information or trade secrets (except documents subject to the Open Records Act).
- Any document marked "confidential," "sensitive," "proprietary," or any document similarly labeled.
- College personnel are encouraged to use common sense judgment in securing the college's confidential information to the proper extent. For example:
    - College personnel, faculty, and students should use common sense and appropriate diligence, and follow other applicable law and/or college policy, in any request/transaction outside the scope of the program that could have information security or identity theft implications: non-financial transaction (e.g., transcript requests, requests for issuance of keys to campus offices, requests to give an employee or student access to a sensitive or confidential database, or access to locked areas).
    - If an employee transports sensitive/non-public information/personal identifying information and needs to leave the vehicle while out, these items and all other sensitive/non-public information/personal identifying information need to be placed out of sight (ex. under seat/in trunk) and vehicle must be locked. All sensitive/non-public information/personal identifying information must be returned to the college location (unless authorized to retain overnight) before leaving for the day. Any sensitive/non-public information retained by employee must be kept inside a secured home/facility overnight. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor/manager.

HARD COPY DISTRIBUTION

Every employee and contractor performing work for the college will comply with the following policies:

- Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday.
- 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.
- When documents containing sensitive information are discarded, they will be placed inside a locked shred bin. Locked shred bins are labeled "Confidential paper shredding and recycling." If you need any assistance in locating one of these bins, please contact a supervisor/manager.

IDENTITY THEFT PREVENTION PROGRAM

Putting the Identity Theft Prevention Program in place enables the college to protect existing students, reducing risk from identity fraud and minimize 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
- Update the program periodically, including reviewing accounts that are covered and identified risks that are part of the program.

The college has a primary relationship with its employees and students other than as a creditor or lender, unlike the creditors/lenders for which the Identity Theft Program was designed. Based on these relationships of employer-employee and student-educational institution, various identity verification measures are already in place under other applicable laws/regulations/programs and should be used consistently (e.g., I-9 employment eligibility verification for employees (with DOB included), National Student Clearinghouse, FAFSA for students, student identification cards/government issued passports/state issued ID and drivers licenses). The Program does not take the place of any such independent requirements.

COVERED ACCOUNTS

Every new and existing customer account that meets the following criteria is covered by this program.

- Business, personal and household information for which there are a reasonably foreseeable risk of identity theft.
- Business, personal and household information for which there are a reasonably foreseeable risk to the safety and/or soundness of the college from identity theft, including financial, operational, compliance, reputation, or litigation risks.

INDICATORS

The following are potential indicators of fraud and should be investigated for verification.

- Suspicious Documents
  - Documents provided for identification appear to have been altered or forged (e.g. lamination from driver's license is not sealed).
  - The photograph or physical description on the identification is not consistent with the appearance of the applicant/student/employee presenting the identification.
  - Other information on the identification is not consistent with information provided by the person opening a new covered account or student/employee presenting the identification (e.g. verbal information is not consistent with printed information).
  - Other information on the identification is not consistent with readily accessible information that is on file with the college, such as a signature card or a recent check.
  - An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- Suspicious Personal Identifying Information
  - Personal identifying information provided by the student/employee is not consistent with other personal identifying information provided by the student/employee. For example: Information collected from the FAFSA and other data collected are inconsistent (William Smith-Bill Smith) Loan information and enrollment information are inconsistent. Students may have multiple/different college ID numbers.
  - Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: The address on an application is the same as the address provided on a fraudulent application.
  - Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the college. For example: The address on an application is fictitious, a mail drop or prison. The phone number is invalid.
  - The SSN provided is the same as that submitted by other persons opening an account or other students/employees.
  - The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other students/employees.
  - The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Unusual Use of, or Suspicious Activity Related to, the Covered Account
  - Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a change of student/employee's name or a new student identification card.
  - A new revolving credit account is used in a matter commonly associated with known patterns of fraud. For example: The student/employee fails to make the first payment or makes an initial payment but no subsequent payments.
  - A covered account is used in a matter that is not consistent with established patterns of activity on the account. There is, for example: Nonpayment when there is no history of late or missed payments.
  - Mail sent to the student/employee is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the student/employee's covered account.
  - The college is notified that the student/employee is not receiving mail.

- Notice from students/employees, victims of identity theft, law enforcement authorities, service providers or other persons regarding possible identity theft in connection with covered accounts held by the college.
    - The college is notified of unauthorized charges or transactions in connection with a student/employee's covered account.
    - The college is notified by a student/employee, a victim of identity theft, a law enforcement authority or any other person that it has opened a fraudulent account for a person engaged in identity theft.
    - Notice to the college of unauthorized access to or use of employee or student account information.
    - There is a breach in the college's computer system security affecting the employee's/student's account or loan.

RESPONDING TO INDICATORS

Once potentially fraudulent activity is detected, it is essential to act quickly as a rapid appropriate response can protect students/employees and the college from damages and loss.

- Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Take this information and present it to the designated authority for determination.
- If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
    - Cancel the transaction
    - Close an affected account and re-open with a new account number
    - Change any passwords or other access codes that permit access to the account
    - Notify actual student/employee that fraud has been attempted
    - Continue to monitor account for evidence of identity theft
    - Notify and cooperate with appropriate law enforcement
    - Determine extent of liability to college
    - Have student/employee complete an Information Discrepancy Affidavit form

PERIODIC UPDATES TO PLAN

- As needed, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current environment.
- Periodic reviews will include an assessment of which accounts are covered by the program.
- As part of the review, indicators may be revised, replaced or eliminated. New indicator 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 students/employees.

PROGRAM ADMINISTRATION

- Involvement of Senior Administration
    - The Identity Theft Prevention Program shall not be operated as an extension to existing fraud prevention programs and its importance warrants the highest level of attention.
    - The Identity Theft Prevention Program is the responsibility of the Board of Trustees. Approval of the initial plan must be appropriately documented and maintained.
    - Operational responsibility of the program can be delegated by the administration.
- Staff Training
    - Staff training shall be conducted for all employees, contractors, consultants, temporary workers, and other workers at the college (volunteers-Student Ambassadors), for whom it is reasonably foreseeable that they may come into contact with accounts or Personally Identifiable Information which may constitute a risk to the college or its students/employees.
    - Staff members shall continue to receive training as required as changes to the program are made to ensure maximum effectiveness of the program.
- Oversight of Service Provider Arrangements
    - It is the responsibility of the college to ensure that the activities of all Service Providers are conducted in accordance with reasonable policies and procedures

designed to detect, prevent, and mitigate the risk of identity theft. If the college engages a service provider to perform an activity in connection with one or more accounts or loans covered by the Program, the college should require, by contract, that the service provider will perform its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft and that the service provider will report any indicators it detects to a member of the college administration with primary responsibility for that service provider relationship.

ROLES AND RESPONSIBILITIES

Administration will have the responsibility to adopt, implement and enforce this policy and ensure that it is followed by employee and contractors. Additional responsibilities regarding the operation of the Identity Theft Prevention Program may be outlined above or as listed in additional written guidance.

DEFINITIONS

Term	Definition
Service Provider	Any person or entity that maintains, processes, or otherwise is permitted access to student/employee information or consumer information through the provision of services directly to the college.
Identity Theft	Fraud committed or attempted by the unauthorized use of personal identifying information of another person.
Personal Identifying Information (PII)	A name or number that can be used alone or with other information to identify a specific person. Ex: Name, SSN, DOB, etc.
Non-Public Information (NPI)	Information that is classified as sensitive information and not available for public display. Ex: Name, Address, Phone Number, SSN, DOB, Driver's License
Indicator	It is a pattern, practice or specific activity that indicates the reasonable possibility of Identity Theft.

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Adopted December 14, 2009
Revised October 18, 2022