MCPHS
IDENTITY THEFT POLICY

SECTION 1: BACKGROUND

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.

SECTION 2: PURPOSE

The College adopts this sensitive information policy to help protect employees and students from damages related to the loss or misuse of sensitive information.

This policy will:

1. Define sensitive information;

2. Describe the physical security of data when it is printed on paper;

3. Describe the electronic security of data when stored and distributed; and

4. Place the College in compliance with state and federal law regarding identity theft protection.

This policy enables the College to protect existing employees and students, reducing risk from identity fraud, and minimize potential damage to the College from fraudulent new accounts. The program will help the College:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;

2. Detect risks when they occur in covered accounts;

3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and

4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

SECTION 3: SCOPE

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

SECTION 4: POLICY

4.A: Sensitive Information Policy

4.A.1: Definition of Sensitive Information

Sensitive information includes the following items whether stored in electronic or printed format:

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

1. Credit card number (in part or whole)

2. Credit card expiration date

3. Cardholder name

4. Cardholder address

4.A.1.b: Tax identification numbers, including:

1. Social Security number

2. Business identification number

3. Employer identification numbers

4.A.1.c: Payroll information, including, among other information:

1. Paychecks

2. Pay stubs

4.A.1.d: Cafeteria plan check requests and associated paperwork

4.A.1.e: Medical insurance information for any employee or student, including but not limited to:

1. Doctor names and claims

2. Insurance claims

3. Any related personal medical information

4.A.1.f: Other personal information belonging to any employee or student, examples of which include:

1. Date of birth

2. Address

3. Phone numbers

4. Maiden name

5. Names

6. I.D. number

4.A.1.g: 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.

4.A.2: Hard Copy Distribution

Each employee and vendor performing work for the College will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

3. 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.

4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.

5. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*" College records may only be destroyed in accordance with the College's records retention policy.

4.A.3: Electronic Distribution

Each employee and vendor performing work for the College will comply with the following policies:

1. Internally, sensitive information may be transmitted using the Colleges e-mail system. All sensitive information must be encrypted when stored in an electronic format.

2. Any sensitive information sent externally must be encrypted and 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."

3. No sensitive information should leave the College (such as via laptop).

SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM

5.A: Covered accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

1. Business, personal and student financial aid account for which there is a reasonably foreseeable risk of identity theft; or

2. 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.

5.B: Credit Reports

5.B.1: 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.

1. Alerts, notifications or warnings from a consumer reporting agency;

2. A fraud or active duty alert included with a consumer report;

3. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or

4. A notice of address discrepancy from a consumer reporting agency.

5.B.2: Red flags also include documentation that indicate a pattern of activity such as:

- A recent and significant increase in the volume of inquiries;

- An unusual number of recently established credit relationships;

- A material change in the use of credit, especially with respect to recently established credit relationships; or

- An account that was closed for abuse of privileges.

5.C: Suspicious documents

5.C.1: Documents provided for identification that appear to have been altered or forged.

5.C.2: A photograph or physical description on an identification that is not consistent with the appearance of the person presenting the identification.

5.C.3: Information on an identification that is not consistent with information provided by a person opening a new covered account.

5.C.4: Other information on an identification that is not consistent with readily accessible information on file with the College, such as a signature on a document.

5.C.5: A document appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5.D: Suspicious personal identifying information

5.D.1: Personal identifying information which is inconsistent with information possessed by the College. For example:

- Aν address does not match any address on file with the College;

- A Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or

- Personal identifying information provided by a person which is not consistent with other personal identifying information provided by such person. For example, there is a lack of correlation between the SSN and date of birth.

5.D.2: Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources. For example, the address on a document is the same as the address provided on a fraudulent document.

5.D.3: Personal identifying information provided is of a type commonly associated with

fraudulent activity as indicated by internal or third-party sources. For example:

- The address on a document is fictitious, a mail drop, or a prison; or

- The phone number is invalid or is a pass through to a pager or answering service.

5.D.4: The SSN provided is the same as that submitted by other persons.

5.D.5: 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.

5.D.6: The person opening a covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

5.D.7: Personal identifying information provided is not consistent with personal identifying information that is on file with the College.

5.D.8: When using security questions (mother's maiden name, pet's name, etc.), the person opening a covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

5.E: Unusual use of, or suspicious activity related to, the covered account

5.E.1: Shortly following the notice of a change of address for a covered account, the College receives a request for the addition of other authorized users.

5.E.2: A new covered account is used in a manner commonly associated with known patterns of fraud patterns. For example, the person fails to make the first payment or makes an initial payment but no subsequent payments

5.E.3: A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example:

- Nonpayment when there is no history of late or missed payments;

- A material change in usage patterns

5.E.4: A covered account that has been inactive for a lengthy period of time is unexpectedly (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

5.E.5: Mail sent to a person is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account.

5.E.6: The College is notified that a person is not receiving paper account statements.

5.E.7: The College is notified of unauthorized charges or transactions in connection with a person's covered account.

5.E.8: The College receives notice from victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the College.

5.E.9: The College is notified by a person, a law enforcement authority, or anyone else that someone has opened a fraudulent account for the purpose of identity theft.

SECTION 6: RESPONDING TO RED FLAGS

6.A: Once a potentially fraudulent activity is detected, the College must act quickly as appropriate to protect students, employees and the College from damages and loss.

6.A.1: 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.

6.A.2: The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

6.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Canceling the transaction;

2. Notifying and cooperating with appropriate law enforcement;

3. Determining the extent of liability of the College or damage to the College; and

4. Notifying the appropriate person that a fraud has been attempted.

5. Notifying any appropriate insurers.

SECTION 7: PERIODIC UPDATES

7.A: 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.

7.B: Periodic reviews will include an assessment of which accounts are covered by the program.

7.C: As part of the review, red flags may be revised, replaced or eliminated. Defining

new red flags may also be appropriate.

7.D: Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the College and its population.

SECTION 8: PROGRAM ADMINISTRATION

8.A: Involvement of management

1. 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.

2. 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 the Executive Vice President.

3. Operational responsibility of the policy is delegated to the Chief Information Officer.

8.B: Staff training

1. 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.

2. The Chief Information Officer is responsible for ensuring identity theft training for all requisite employees and vendors.

3. Employees must receive annual training in all segments of this policy.

4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

8.C: Oversight of Vendor arrangements

1. 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.

2. 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.

3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.