PROCEDURE 2.16.1: IDENTITY THEFT PREVENTION

The risk to the district, its employees and customers 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 contractor.

Under the Red Flags Rule, the college is required to establish an identity theft prevention program tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify potentially fraudulent activity within new or existing covered accounts.
2. Detect risks when they occur in covered accounts.
3. Respond appropriately to detected risks to prevent and mitigate identity theft.
4. Update the program periodically to reflect changes in identity theft risks to students and other college constituents.

The college-appointed internal information security awareness committee will oversee, train and update the identity theft prevention program.

In June 2015, the Red, Yellow and Green Document Classification procedure was put in place and is summarized as follows:

Red

Documents containing sensitive/confidential information, including personally identifiable information (PII) always needs to be saved as red. PII, as used in U.S. privacy law and information security, is information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context. These documents are stored on a local file server and can be accessed only from campus.

Yellow

Documents that aren't sensitive or confidential but are internal and not public information are stored on SharePoint team sites in Office 365 and are made accessible via sharing permission to authorized faculty and staff.

Green

These are public documents viewable on the college website.

Identity theft prevention program

This identity theft prevention program was developed pursuant to the Federal Trade Commission's Red Flag Rule.

Section 1: purpose

The college adopts this sensitive information program to help protect employees, customers, contractors and the college from damages related to the loss or misuse of sensitive information.

This program:

1. Defines sensitive information.
2. Places the college in compliance with state and federal law regarding identity theft protection.

This program enables the college to protect existing customers, reducing risk from identity fraud, and minimize potential damage to the college from fraudulent new accounts. The program helps 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.
4. Update the program periodically, including reviewing the accounts covered and the identified risks that are part of the program.

Section 2: scope

This protection program applies to employees, contractors, consultants, temporary workers and other workers at the college, including all personnel affiliated with third parties.

Section 3: definitions

IDENTITY THEFT

A 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

Any student accounts or loans administered by the college.

CHIEF INFORMATION OFFICER

The individual designated with primary responsibility for oversight of the program. See Section 8 below.

IDENTIFYING INFORMATION

Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, phone 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, internet protocol address or routing code.

SENSITIVE INFORMATION

The following items stored in electronic or printed format:

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

Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification numbers

Payroll information, including, among other information:

1. Paychecks
2. Pay stubs

Cafeteria plan check requests and associated paperwork.

Medical information for any employee or customer, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

Other personal information belonging to any customer, employee or contractor, examples of which include:

1. Date of birth
2. Address
3. Phone numbers

4. Maiden name
5. Name(s)
6. Customer number

College personnel are encouraged to use common-sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, they should contact their supervisor.

Section 4: identification of red flags

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.

NOTIFICATION AND WARNINGS FROM CREDIT REPORTING AGENCIES

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

SUSPICIOUS DOCUMENTS

1. Documents provided for identification that appear to have been altered or forged.
2. The photograph or physical description on the identification isn't consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification isn't consistent with:
   a. Existing student/employee information
   b. Readily accessible information on file with the college
4. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

SUSPICIOUS PERSONAL IDENTIFYING INFORMATION (PII)

1. Provided personal identifying information (PII) is:
   a. Inconsistent with other information the student provides (e.g., inconsistent birth dates)
   b. Inconsistent with other sources of information (for instance, an address not matching an address on a loan application)
   c. The same as information shown on other applications that were found to be fraudulent
2. Identifying information presented that's consistent with fraudulent activity (such as an invalid phone number or fictitious billing address)
3. The SSN provided is the same as one given by another student.
4. The address or phone number provided is the same as or similar to the address or phone number of another person.

5. The customer or the person opening the covered account fails to provide all required PII on an application or in response to notification that the application is incomplete.
6. Provided PII is not consistent with personal identifying information on file with the college.

UNUSUAL USE OF, OR SUSPICIOUS ACTIVITY RELATED TO, THE COVERED ACCOUNT

1. Shortly following the notice of a change of address for a covered account, the college receives a request to change the student's name.
2. Payments stop on an otherwise consistently up-to-date account.
3. A covered account is used in a manner inconsistent with established patterns of activity on the account.
4. Mail sent to the student is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the student's covered account.
5. The college is notified that the student isn't receiving mail sent by the college.
6. The college is notified of unauthorized charges or transactions in connection with a student's covered account.
7. Breach in the college's computer system security.
8. Unauthorized access to or use of student account information.

ALERTS FROM OTHERS

1. Notice to the college from a student, identity theft victim, law enforcement or other person the college has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Section 5: detecting red flags

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:

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

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:

1. Verify the identification of student if they request information (in person, via phone, via email).
2. 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.

3. Verify changes in banking information given for billing and payment purposes.

Section 6: preventing and mitigating identity theft

In the event college personnel detect any identified red flags, they'll take one or more of the following steps, depending on the degree of risk posed by the red flag:

1. Continue to monitor a covered account for evidence of identity theft.
2. Cancel the transaction.
3. Contact the student or applicant.
4. Change any passwords or other security devices that permit access to covered accounts.
5. Not open a new covered account.
6. Provide the student with a new student identification number.
7. Notify the chief information officer for determination of the appropriate step(s) to take.
8. Notify law enforcement.
9. File or assist in filing a suspicious activities report (SAR).
10. Determine that no response is warranted under the particular circumstances.

To further prevent the likelihood of covered account identity theft, the college will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure its website is secure or provide clear notice that the website is not secure.
2. Ensure file cabinets, desk drawers and any other storage spaces or rooms containing documents with identifying information be locked when not in use or unsupervised.
3. Ensure desks, workstations, printers, copiers, fax machines, whiteboards, dry-erase boards in common shared work areas are cleared of all identifying information when not in use.
4. 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 (in accordance with the college's records retention policy).
5. Ensure office computers with access to covered account information are password protected.
6. Internally, sensitive information may be transmitted using approved college e-mail. All sensitive information must be encrypted when stored in an electronic format.
7. Any sensitive information sent externally must be encrypted and password protected. Additionally, a statement such as this 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."
8. Avoid use of Social Security numbers.
9. Ensure computer virus protection is up to date.
10. Require and keep only the kinds of student information necessary for college purposes.

Section 7: program administration

Responsibility for developing, implementing and updating the program lies with an internal information awareness committee.

STAFF TRAINING

1. Staff training is conducted for all employees.
2. The chief information officer, together with Human Resources, is responsible for ensuring identity-theft training for all requisite employees and contractors.
3. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.
4. College employees are expected to notify the chief information officer once they become aware of an identity theft incident or the college's failure to comply with this program.

SERVICE-PROVIDER ARRANGEMENTS

1. The college ensures 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.
2. A service provider 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 meet these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

NON-DISCLOSURE OF SPECIFIC PRACTICES

For the effectiveness of this program, knowledge about specific red flag identification, detection, mitigation and prevention practices may need to be limited to the committee who developed this program and to those employees with a need to know them. Any documents produced to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential and shouldn't be shared with the public. The chief information officer will inform the committee and those employees with a need to know of those confidential documents or specific practices.

PERIODIC UPDATES TO PLAN

The committee will periodically review and update the program to reflect changes in risks to students and the soundness of the college from identity theft, considering the college's experiences with identity-theft situations, changes in identity-theft methods, changes in identity-theft detection and prevention methods, and changes in the college's business arrangement with other entities. After considering these factors, the chief information officer will determine whether changes to the program, including listing the red flags, are warranted., and if so, update the program. At periodic intervals established in the program, or as required,

the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

Original: 4/10
Reviewed: 5/16, 12/17, 1/18, 1/24
Revised: 5/16,12,17, 1/18, 1/24