17.1 Background

The risk to Clayton State University (herein referred to as University), its employees and customers from data loss and identity theft is of significant concern to the University and can be reduced only through the combined efforts of every employee and contractor.

17.2 Purpose

The University adopts this sensitive information policy to help protect employees, students, customers, its contractors and the University 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 University in compliance within the state and federal law regarding identity theft protection.

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

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

17.2.1 Scope

This policy and protection program applies to employees, contractors, consultants, temporary workers, and other workers of the University.

17.3 Definitions

17.3.1 Sensitive Information

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

1. Credit Card information including:
    a. Credit card number (in part or whole),
    b. Credit card expiration date,
    c. Cardholder name, and
    d. Cardholder address
2. Tax identification numbers including:
    a. Social Security number
    b. Business identification number
    c. Employer identification numbers
3. Payroll information including but not limited to:
    a. Paychecks
    b. Paystubs
4. Medical Information for any employee, temporary worker, student, customer including but not limited to:
    a. Doctor names and claims
    b. Insurance claims
    c. Prescriptions
    d. Any related personal medical information
5. Other personal information belonging to any employee, temporary worker, student and customer, examples of which include:
    a. Date of birth
    b. Address
    c. Phone numbers
    d. Maiden or birth name(s)
    e. Student or Customer number
6. University 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, s/he should contact their supervisor.

17.3.2 Hard Copy Distribution

Each employee and contractor performing work for the University 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 work day 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 areas will be erased, removed, or paper 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 shredding device. Locked shred bins are labeled *"Security Container.*" University records, however, may only be destroyed in accordance with the Board of Regents and the University's records retention policies.

17.3.3 Electronic Distribution

Each employee and contractor performing work for the University will comply with the following policies:

1. Internally, sensitive information may be transmitted using approved University e-mail. When feasible, all sensitive information must be encrypted when stored in an electronic format.

2. Any sensitive information sent both internally and externally must be encrypted and password protected and sent only to approved recipients. 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 which it was originally addressed. Any use by others is strictly prohibited."

17.4 Red Flags

17.4.1 Red Flags Rule Definitions

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

A “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”

A “Covered Account” includes all student accounts or loans that are administered by the University.

“Program Administrator” is the individual designated with primary responsibility for oversight of the program.

“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, 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, computer’s Internet Protocol address, or routing code.

17.4.2 Identification of Red Flags

In order to identify relevant Red Flags, the University 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 experiences with Identity Theft. The University identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies – Red Flags

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

B. Suspicious Documents – Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;

2. Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document;

3. Other document with information that is not consistent with existing student information; and

4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information - Red Flags

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);

2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another student;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. A person’s identifying information is not consistent with the information that is on file for the student.

D. Suspicious Covered Account Activity or Unusual Use of Account –Red Flags

1. Change of address for an account followed by a request to change the student’s name;

2. Payments stop on an otherwise consistently up-to-date account;

3. Account used in a way that is not consistent with prior use;

4. Mail sent to the student is repeatedly returned as undeliverable;

5. Notice to the University that a student is not receiving mail sent by the University;

6. Notice to the University that an account has unauthorized activity;

7. Breach in the University's computer system security; and
8. Unauthorized access to or use of student account information.

E. Alerts from Others – Red Flags

1. Notice to the University from a student, Identity Theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

17.4.3 Detecting Red Flags

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, University 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; and
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).

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

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

C. Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and

2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

17.4.4 Preventing and Mitigating Identity Theft

In the event University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Notify your supervisor for determination of the appropriate step(s) to take;

2. Change any passwords or other security devices that permit access to Covered Accounts;

3. Contact the student or applicant (for which a credit report was run);

4. Provide the student with a new student identification number;

5. Continue to monitor a Covered Account for evidence of Identity Theft;

6. Notify law enforcement;

7. Not open a new Covered Account;

8. File or assist in filing a Suspicious Activities Report ("SAR"); or

9. Determine that no response is warranted under the particular circumstances.

17.4.5 Protect Student Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;

2. 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;

3. Ensure that office computers with access to Covered Account information are password protected;

4. Avoid use of social security numbers;

5. Ensure computer virus protection is up to date; and

6. Require and keep only the kinds of student information that are necessary for University purposes.

17.5 Program Administration

17.5.1 Oversight

Responsibility for developing, implementing and updating this Program lies with Business and Operations for the University. The Program Administrator may be the Vice President of Business and Operations or his or her appointee. The Program Administrator will be responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

17.5.2 Staff Training and Reports

University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify their supervisor who in turn will notify the Program Administrator once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program.

17.5.3 Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require by contract, that service providers have such policies and procedures in place; and

2. Require by contract, that service providers review the University's Program and report any Red Flags to the Program Administrator or the University employee with primary oversight of the service provider relationship.