MIDWESTERN STATE UNIVERSITY

# Operating Policies & Procedures Manual

## University Operating Policy/Procedure (OP)
## OP 62.06: Identity Theft Prevention Program

| | |
|---|---|
| **Approval Authority:** | President |
| **Policy Type:** | University Operating Policy and Procedure |
| **Policy Owner:** | Vice President for Administration and Finance |
| **Responsible Office:** | Controller’s Office |
| **Next Scheduled Review:** | 12/01/2021 |

### A. Program Adoption

This policy was developed pursuant to the Federal Trade Commission's Red Flags Rule (“Rule”), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

### B. Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account, and to provide for continued administration of the program. The program shall include reasonable policies and procedures to:

1. identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
2. detect red flags that have been incorporated into the program;
3. respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. ensure the program is updated periodically to reflect changes in risks to students, staff, or faculty and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

### C. Definitions

1. Identity Theft: Fraud committed or attempted using the identifying information of another person without authority.
2. Red Flag: Pattern, practice, or specific activity that indicates the possible existence of identity theft.
3. Covered Account: An account offered by or maintained by the university involving or permitting multiple payments or transactions, including extension of credit or a deposit account. Examples: Installment payments for tuition accounts, emergency loans, One Card.

4. Program Administrator: The individual designated with primary responsibility for oversight of the program. See Section H below.
5. Identifying information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. Examples: 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, staff, or faculty identification number, computer's Internet Protocol address, or routing code.

## D. Identification of Risk Factors

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. Areas must be identified where there is a potential for identify theft. The program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The types of covered accounts as noted above;
2. The information required to open covered accounts:
   a. Common application with personally identifying information
   b. Bank information
   c. High school/previous college transcript
   d. Official ACT or SAT scores
   e. Letters of recommendation
   f. Entrance medical record
   g. Medical history
   h. Immunization history
   i. Insurance information
   j. Background check
   k. Educational background
   l. Educational certification
3. The methods provided to access covered accounts:
   a. ID's and passwords for web based transactions.
   b. Photo identification for in-person transactions.
   c. Information sent to individuals via provided e-mail based information.
4. The university's previous history of identity theft.

## E. Identification of Red Flags

The university identifies the following red flags:

1. A request to mail something to an address not listed on file
2. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
3. Notifications and Warnings from Credit Reporting Agencies
   a. Report of fraud accompanying a credit report;
   b. Notice or report from a credit agency of a credit freeze on an applicant;
   c. Notice or report from a credit agency of an active duty alert for an applicant;
   d. Receipt of a notice of address discrepancy in response to a credit report request; and
   e. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.
4. Suspicious Documents

   a. Documents provided for identification appear to have been altered, forged or inauthentic;
   b. The photograph or physical description on the identification is not consistent with the appearance of the student, staff, or faculty presenting the identification;
   c. Other document with information that is not consistent with existing student, staff, or faculty information; and
   d. Application for service that appears to have been altered or forged.
5. Suspicious Personal Identifying Information
   a. Identifying information presented that is inconsistent with other information the student, staff, or faculty provides (example: inconsistent birth dates);
   b. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
   c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
   d. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
   e. Social security number presented that is the same as one given by another student, staff, or faculty, or is unissued or listed on the SSA’s Death Master File;
   f. An address or phone number presented that is the same as that of another person;
   g. A person fails to provide complete personal identifying information on an application when reminded to do so; and
   h. A person’s identifying information is not consistent with the information that is on file for the student, staff, or faculty. For example, there is a lack of correlation between the SSN range and date of birth.
6. Unusual use of the covered account.
   a. Change of address for an account followed by a request for replacement card or addition of authorized user.
   b. Payments stop on an otherwise consistently up-to-date account;
   c. Account used in a way that is not consistent with prior use (example: very high activity);
   d. Mail sent to the account holder is repeatedly returned as undeliverable;
   e. Notice to the university that a customer is not receiving mail sent by the university;
   f. Notice to the university that an account has unauthorized activity;
   g. Breach in the university's computer system security; and
   h. Unauthorized access to or use of customer account information.
7. Alerts from Others

   Notice to the university from a student, staff, or faculty 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.

## F. Detecting Red Flags

1. 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:

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

2. 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:

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

3. 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:

   a. 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
   b. 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.

## G. 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. Continue to monitor a covered account for evidence of identity theft;
2. Deny access to the covered account until other information is available to eliminate the red flag;
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, faculty, or staff with a new identification number;
7. Notify the program administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement;
9. File or assist in filing a Suspicious Activities Report ("SAR"); or
10. Determine that no response is warranted under the particular circumstances.

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.

## H. Program Administration

1. Oversight

Responsibility for developing, implementing and updating this program lies with the Vice President for Business Affairs and Finance. The program administrator will be responsible for the program administration, for ensuring appropriate training of university staff, 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.

1. Staff Training and Reports

University staff responsible for implementing the program shall be trained either by or under the direction of the program administrator in the detection of red flags and the responsive steps to be taken when a red flag is detected. University staff shall be trained, as necessary, to effectively implement the program. University employees are expected to 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. At least annually or as otherwise requested by the program administrator, university staff responsible for development, implementation, and administration of the program shall report to the program administrator on compliance with this program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of covered accounts, service provider arrangements, significant incidents involving identity theft and management’s response, and recommendations for changes to the program.

2. 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.

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

b. 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.

3. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific red flag identification, detection, mitigation and prevention practices may need to be limited to the committee that developed this program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered “confidential” and should not be shared with other university employees or the public. The program administrator shall inform the committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

4. Program Updates
   The committee will periodically review and update this program to reflect changes in risks to students and the soundness of the university from identity theft. In doing so, the committee will consider the university's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the university's business arrangements with other entities. After considering these factors, the program administrator will determine whether changes to the program, including the listing of red flags, are warranted. If warranted, the committee will update the program.

## Responsible Office

Contact:
Phone:
Email:

## Revision History

05/15/2009: MSU Policy 4.132 (Identity Theft Prevention Program is adopted by the MSU Board of Regents as MSU Policy and Procedure. 4.132)