

## **Governing Policy: Identity Theft**

### **Policy Statement:**

The Missouri State University Board of Governors approves the creation of the Identity Theft Policy and establishes an Identity Theft Program to formally develop reasonable policies and procedures to comply with The Fair and Accurate Credit Transactions Act of 2003 as amended (FACT Act).

### **Purpose of the Policy:**

The Identity Theft Policy is designed to establish an Identity Theft Prevention Program which shall develop reasonable procedures covering the following four elements:

- Identify relevant Red Flags(as defined in the FACT ACT) for Covered Accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft;
- Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

### **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 Identify Theft.”

A “Covered Account” includes all student, faculty and staff accounts, extensions of credit 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 but not limited to: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, passport number, student identification number.

### **Covered Accounts**

University has identified the following types of accounts which are Covered Accounts:

1. Participation in Federal Perkins Loan Program
2. Zip Cards which allow Institutional loans to students, faculty and staff
3. Extensions of credit including payment plans

### **Identity Theft Program Committee:**

The Identity Theft Program committee shall develop the Identity Theft Program. The following areas will be represented on the committee: Student Affairs, Administrative and Information Services, West Plains, Computer Services and Financial Services, General Counsel (ex officio).

The Committee shall develop procedures for the following:

- Detect Address Discrepancies
- Detect, prevent, and mitigate identify theft
- Provide training to appropriate staff
- Develop procedures including validity of changes of address as it relates to Red Flags.

The Identity Theft Program Committee shall take into consideration and address the potential for identity theft by incorporating any or all of the following:

- Alerts, Notifications or Warnings from a Consumer Reporting Agency;
- Suspicious Documents;
- Suspicious Personal Identifying Information;
- Information defined as Restricted Information under the Data Classification Policy
- Unusual Use of, or Suspicious Activity Related to, the Covered; and
- Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

### **Periodic Updates to Plan:**

At periodic intervals established by the Identity Theft Program Committee, 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. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

**Program Administration:**

The President may revise, replace or eliminate provisions of this policy or the Identity Theft Program as appropriate. Operational responsibility of the program is delegated to the Chief Financial Officer who shall be the Program Administrator. (Res. Policies & Procedures No. 134-09; Bd. Min. 5-14-09)