65-8 Identity Theft

1. **Purpose.** The purpose of this policy, procedures and the Identity Theft Plan (the Plan) is to establish processes 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 continues administration of the plan in compliance with 16 C.F.R. Part 681. The policy complies with the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

2. **Policy.** This policy enables Eastern New Mexico University System (the System) to protect consumers, reduce risk from identity fraud and minimize potential damage to the System from fraudulent new accounts. The policy, which also authorizes the "Identity Theft Protection Plan," shall address the following:

   A. Identity relevant Red Flags for new and existing covered account and incorporate those Red Flags into the Plan;

   B. Detect Red Flags that have been incorporated into the Plan;

   C. Respond appropriately to any Red Flags that are detected to present and mitigate identity theft, and

   D. Ensure the Plan is updated periodically to reflect changes in risks to students or employees of the System to ensure their safety from identity theft.

The forgoing policies, procedures and Plan shall be implemented using the following:

Guidelines and Procedures

3. **Administration.** These policies, procedures and the Plan shall be administered by the ENMU System chief financial officer (CFO) or his or her designee.

4. **Definitions.**

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

   B. "Red Flag" is a pattern, practice or special activity that indicates the possible existence of identity theft.

   C. A "covered account" includes all students or employee accounts that are designed to permit multiple payments or transactions, including student loans, and which are administered by the System.

   D. "Identifying information" is any name or number that may be used alone or in conjunction with any other information to identity a specific person, including name, address, telephone number, social security number, date of birth, driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number, students identification number, credit card information, computer's Internet Protocol (IP) address, or routing number.

5. Plan Administration.

A. **Oversight.** The Plan administrator with responsibility for implementing this policy and for developing, implementing and updating the Plan is the CFO or his /her designee, assisted by a committee appointed by the CFO. The Plan administrator shall be responsible for ensuring appropriate training of all staff and faculty, reviewing any reports regarding the detection of Red Flags and determining the steps for preventing and mitigating identity theft. The administrator shall direct that periodic reviews of the Plan be conducted as needed updates and improvements.

B. **Staff Training and Reports.** System staff responsible for implementing the Plan shall be trained in the detection of Red Flags and the steps to be taken when a Red Flag is detected. System staff shall be trained, as necessary, to effectively implement the Plan. Annually, or as requested by the Plan administrator, the staff responsible for administration of this plan shall report to the Plan administrator on compliance with the Plan.

C. **Service Provider Arrangements.** In the event the System engages a service provider to perform an activity in connection with one or more covered accounts, the System shall ensure the service provider perform its activity in accordance with policies and procedures designed to detect, prevent and mitigate the risk of identity theft as detailed in the Identity Theft Prevention Plan.

D. **Non-Disclosure of Specific Practices**. Knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the committee appointed to over Plan implementation and those employees with a need to know them. Documents produced or developed that describe such specific practices are considered confidential and should not be shared with other employees or the public.

E. **Plan Updates.** The committee shall periodically review and update the Plan to reflect changes in risks to students, employees, and the soundness of the System from identity theft.

6. The Identity Theft Prevention Plan. The System shall maintain and implement an Identity Theft Prevention Plan that describes the procedures, for assuring the security of covered accounts and the implementation of practices that prevent identity theft in any form.

Approved by the Board of Regents on April 28, 2009.
Approved by the Board of Regents June 1, 2019