EWU Policy 202-08

Effective April 27, 2009

University Operations – Financial Activities

Identity Theft Prevention Program

History: This publication is new. It was adopted by the Board of Trustees on June 25, 2009. It finalizes Interim Policy 203-02 that was adopted by the University President on April 27, 2009. Renumbered from EWU 202-02 on June 22, 2011.

Summary: This policy establishes and describes the Identity Theft Prevention Program for Eastern Washington University.

Applicability: This policy applies to all faculty, staff, and students of Eastern Washington University.

Proponent: The proponent of this policy is the Vice President for Business and Finance.

Authority: The authority for establishment and modification of this policy is the EWU Board of Trustees (BOT). Changes to this policy must be approved by the BOT and must conform to the procedures for changing policies contained in EWU Policy 201-01.

Delegation: The Board of Trustees delegates authority for addition and modification of appendices to this policy to the Vice President for Business and Finance. Delegation authority includes resultant changes to the table of contents.

Review: This policy will be reviewed every five years.

Supplementation:
Supplementation is authorized, so long as any such supplementation does not conflict with university level policy or higher authority.

Suggested improvements: Users are invited to send comments and suggested improvements to:

Office of the President
ATTN: Policy Administrator
Eastern Washington University
214 Showalter Hall
Cheney, WA 99004

CONTENTS

CHAPTER 1
GENERAL

1-1. Purpose

This policy establishes standards for the protection of personal information and the prevention of identity theft for students and employees of Eastern Washington University.

1-2. Background

Eastern Washington University developed this policy to address prevention, detection, and mitigation of identity theft pursuant to the Federal Trade Commission's (FTC) Red Flags Rule as defined in sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT) of 2003.

The Fair and Accurate Credit Transactions Act (FACT) requires that this policy be adopted by the Board of Trustees and overseen by senior management. Oversight includes routine reports from staff regarding compliance with the act as well as changes to the policy that are made from time to time to address changes in risk. Staff members who are involved in opening and handling covered accounts must be trained to identify risks and how to respond to them.

1-3. 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, loans or Eagle Cards that are administered by Eastern Washington 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. This information includes: 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.

CHAPTER 2
IDENTITY THEFT PREVENTION

2-1. Red Flags

In order to identify 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. Department managers and supervisors will take appropriate measures to identify specific Red Flags that may indicate potential identity theft activities relative to shared accounts at the University. The following are general examples of Red Flags which may indicate fraudulent activity.

a. Notification and warnings from credit reporting agencies

b. Suspicious documents

c. Suspicious account activity

d. Alerts from others

2-2. Detecting Red Flags

University personnel will take appropriate measures to detect identified red flags. Department managers and supervisors will share information regarding identified Red Flags and related detection measures with appropriate personnel within their departments. Examples of detection measures, based on common Red Flags for EWU, include:

a. Identity and Information Verification

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification prior to taking any action or providing any information relative to student accounts.

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).

3. Verify the student’s identity if they request information (in person via telephone, facsimile, email).

4. 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.

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

b. Consumer (“Credit”) Report Requests

1. When a notification or warning from a credit reporting agency is received, university officials will take appropriate actions to verify account information and to resolve any discrepancies.

2-3. Preventing and Mitigating Identify Theft

a. Preventing Identity Theft: In order to prevent the likelihood of identity theft from occurring with respect to Covered Accounts, University personnel will take appropriate measures to protect student identifying information. Such measures may include:

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

2. Ensure complete 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 computers with access to covered account information are password protected.

4. Restrict access to social security numbers except where legally required.

5. Ensure computer virus protection is up to date on all computers

6. Require and keep only the student information that is necessary for University purposes.

b. Mitigating Threats of Identity Theft: In the event University personnel detect an identified Red Flag, department managers and supervisors will direct appropriate response measures, depending on the degree of risk posed, to prevent and/or mitigate the effects of identity theft. Such measures may include:

   1. Continue to monitor a covered account for evidence of identity theft.

   2. Contact the covered account holder for which a credit report was run.

   3. Change any passwords or other security devices that permit access to covered accounts.

   4. Not open a new covered account for the account holder.

   5. Provide the student or customer a new EWU identification number.

   6. Contact the administrator of the program to determine appropriate response measures.

   7. Notify law enforcement.

   8. File or assist in filing a report of the suspicious activity or determine that no response is warranted under the particular circumstances.

2-4. Program Administration

Oversight, administration, training, reporting and program updates will reside with the Business and Finance division of the university. This includes developing procedures, as needed, for the identification, detection, prevention and mitigation of Red Flags.

Staff responsible for implementation shall be trained by the program administrator in the detection of Red Flags and the steps to be taken when a Red Flag is detected. University employees are expected to notify the program administrator once they become aware of an incident of identity theft.

A periodic review and update of this program will be done, as needed, to reflect changes in risks to customers. After considering proposed changes, the program administrator will determine whether changes to the program are warranted.

The Information Security policy and related guidance will be referred to for information relative to information technology practices and security measures related to covered accounts as described in this policy.