Identity Theft Prevention Program

University Operations – Financial Activities

EWU Policy 202-08 | **Authority: EWU Board of Trustees**

Effective: June 22, 2023 | **Proponent: Vice President for Business & Finance**

Summary: This policy establishes and describes the identity theft prevention program for Eastern Washington University.

History: This policy revises the previous version dated June 25, 2009, which was renumbered in June 2011 and reformatted in February 2023. It was approved by the Board of Trustees on June 22, 2023.

Applicability: This policy applies to all Eastern Washington University accounts covered by Fair Credit Reporting Act.

1. GENERAL

1-1. Purpose

This policy establishes standards for the detection, prevention, and mitigation of identity theft involving covered university accounts 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) Identify Theft Rules as defined in the Fair Credit Reporting Act (16 CFR part 681).

The Fair Credit Reporting Act 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.

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. The university Chief Information Officer, or designee, serves as the Program Administrator for EWU.

"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.

2. IDENTITY THEFT PREVENTION

2-1. Identifying Red Flags

To identify relevant Red Flags for its Covered Accounts, the University considers the types of accounts that it offers and maintains, methods it provides to open accounts, methods to access accounts, and previous experiences with Identity Theft.

Departments who manage Covered Accounts shall identify more specific Red Flags, as needed, for their respective Covered Accounts.

The following are general examples of Red Flags that may indicate fraudulent activity:

a. Notification and warnings from credit reporting agencies, such as fraud detection services;
b. Suspicious documents or presentation of suspicious personal identifying information such as a suspicious address change;
c. Unusual use of or other suspicious account activity;
d. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft connected to a Covered Account.

2-2. Detecting Red Flags

Departments who manage Covered Accounts shall ensure appropriate staff are trained to detect and report identified Red Flags.

Departments shall also implement measures to facilitate detection of Red Flags and ensure staff are informed of those measures. 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, home address or other identification prior to taking any action or providing any information relative to student or employee accounts.

2. Verify the user's identity at time of issuance of student identification card (review of driver's license

or other government-issued photo identification).

3. Verify the user's identity if they request information in person by telephone.

4. Verify the validity of requests to change billing addresses by mail or email and provide the user 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

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 Identity Theft

a. Preventing Identity Theft: All university departments shall comply with the information security and privacy requirements of EWU Policy 203-01. Departments who manage Covered Accounts shall also take appropriate measures to protect student identifying information and prevent identity theft, including:

1. Emphasize and enforce data minimization, requiring and keeping only the information that is necessary to fulfill university requirements.

2. . Store protected information only in secure and appropriate systems.

3. 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.

4. Ensure that computers with access to covered account information are password protected and require multi-factor authentication for access.

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

6. Ensure computer virus and malware protection is up to date on all computers.

b. Mitigating Threats of Identity Theft: If there is any reason to believe there may have been unauthorized access to a covered account, departments must follow the Unauthorized Disclosures and Breach Notifications procedures per Chapter 4 of EWU Policy 203-01, Information Security.

2-4. Program Administration

The Program Administrator is responsible for oversight, administration, training, reporting and updates to the Identity Theft Prevention Program.

Staff in departments who manage Covered Accounts shall be trained, as necessary, to effectively implement this program.

The Program Administrator shall periodically review and update this program to reflect changes in risks to customers and to the university's methods and procedures for preventing and responding to identify theft.

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.