PROCEDURE NAME: **6.8 Identity Theft Red Flag Compliance Plan**

Reference: Fair and Accurate Credit Transactions Act (Pub. L 108-159) Section 114

**Note:** This procedure is legally required. It addresses the Chaffey Policy: Chapter 6: Business/Financial Affairs, 6.8 Identity Theft Red Flag Compliance Plan

No covered accounts are currently maintained by Chaffey College.

**Purpose:** To establish an Identity Theft Red Flag Compliance Plan designed to detect, prevent, and mitigate identity theft in the event that the District opens or maintains a covered account, and to provide for continued administration of the Plan to:

- Identify relevant red flags for covered accounts offered and maintained and incorporate those red flags into the Plan;
- Detect red flags that have been incorporated into the Plan;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft;
- Ensure the Plan is updated periodically to reflect changes in risk related to students/employees and the safety and soundness of the practices to prevent identity theft;
- Incorporate existing policies and procedures that control reasonably forecasted risks (as appropriate).

1. **Plan Adoption.** Chaffey College ("College") developed this Identity Theft Red Flag Compliance Plan ("Plan/Procedure") 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.

2. **Definitions.**

   2.1 Identity theft means fraud committed or attempted using the identifying information of another person without authority.

   2.2 A red flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

   2.3 A covered account means an account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

3. **Identification of Red Flags.** The Plan/Procedure considers the following risk factors in identifying relevant red flags for covered accounts:

   3.1 The types of covered accounts the College offers or maintains;
3.2 The method of opening a covered account;

3.3 The method for accessing a covered account;

3.4 The method for maintaining a covered account;

3.5 The College’s previous experience with identity theft.

4. Sources of Red Flags.

4.1 The Plan/Procedure identifies the following red flags:

   a. Documents provided for identification appear to have been altered or forged;

   b. The photograph or physical description on an identification card is not consistent with the appearance of the student/employee presenting the identification;

   c. Receipt of notification regarding possible identity theft in connection with a covered account.

4.2 The College will continue to incorporate relevant red flags into this Plan/Procedure from the following sources:

   a. Incidents of identity theft that the College has experienced;

   b. Methods of identity theft that the College identifies that reflects changes in identity theft risks;

   c. Guidance from the College’s supervisors who identify changes in identity theft risks.

5. Detection of Red Flags.

5.1 The College employs practices to safeguard credit activities, which includes refund of a credit balance. Refunds of credit balances are automatically processed each term and either mailed to the address on file or refunded to the credit card.

5.2 In the event the College begins to maintain covered accounts, this Plan/Procedure will be updated to further address aiding in the detection of red flags.
6. Response to Red Flags. To prevent and mitigate identity theft once a covered account is maintained by the College, the appropriate responses to the relevant red flags should be followed:

6.1 Deny access to the covered account until other information is available to eliminate the red flag;
6.2 Notify the student or employee whose account is being accessed using the information on file;
6.3 Recommend any passwords, security codes, or other security devices that permit access to a covered account be changed as appropriate;
6.4 Notify law enforcement or the Administrator responsible for student/employee discipline; or,
6.5 Determine no response is warranted under the particular circumstances.

7. Oversight/Updating of the Plan/Procedure. The Vice President of Administrative Services (“Plan Administrator”) is responsible for developing, implementing, updating, and administering the Plan/Procedure and will ensure adherence to following steps:

7.1 Appropriate training of the College’s staff on the Plan/Procedure;
7.2 Reviewing any staff reports regarding the detection of red flags;
7.3 Reviewing the steps for preventing and mitigating identity theft;
7.4 Determining which steps of prevention and mitigation should be taken in particular circumstances; and,
7.5 Considering annual changes to the Plan/Procedure to address changing identity theft risks.

8. Staff Training. College staff responsible for implementing the Plan/Procedure will be trained either by or under the direction of the Plan Administrator in the detection of Red Flags, and the responsive steps to be taken when a red flag is detected.