



POLICY: 6Hx28:7B-06

Responsible Executive: Chief
Information Officer

Policy Contacts: Managing Director,
CISO

Specific Authority: 1001.64, F.S.

Law Implemented: Red Flags Rule (16
C.F.R. § 681)

Effective Date: 09-11-2025

Date of Last Policy Review:
09-11-2025

Identity Theft Prevention Program

Policy Statement:

- I. Valencia College (“College”) is committed to detect, prevent, and mitigate identity theft when conducting College business in compliance with the Federal Trade Commission’s Red Flag Rule. The College’s Identity Theft Prevention Program (“Program”) shall include reasonable procedures to:
 - A. Determine the applicability of Red Flags Rules to the College;
 - B. Identify relevant Red Flags for covered accounts it offers or maintains and incorporate those Red Flag(s) into the Program;
 - C. Detect Red Flags that have been incorporated into the Program;
 - D. Respond appropriately to any Red Flag(s) that are detected to prevent and mitigate identity theft; and
 - E. Ensure the Program is reviewed and updated periodically as appropriate to reflect changes in risks to students, employees, and creditors from identity theft.
- II. The College President shall designate a College official to serve as Program Administrator responsible for exercising appropriate and effective oversight over the Program and the Program Administrator shall regularly report to the College President on the effectiveness of the Program along with any recommended changes for approval. The President’s approval shall be sufficient to make changes to the Program.
- III. The College President or designee(s) may adopt procedures to implement this policy.

Policy History: Adopted 9-11-25

Related Documents/Policies:

College Policy 6Hx28: 1-10 Policy Against Improper Activities; Whistleblower Protection

College Policy 6Hx28: 7A-01 Information Security Program

College Policy 6Hx28: 3E-08 Disciplinary Action

College Policy 6Hx28: 7B-04 Financial Information Security Program

College Policy 6Hx28: 8-03 Student Code of Conduct

Procedures:

I. Definitions:

A. Covered accounts:

1. Any account the College offers or maintains primarily for personal, family or household purposes, which involves multiple payments or transactions.
2. Any other account the College offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College from Identity Theft.

B. Credit: The right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefor.

C. Creditor: An entity that regularly extends, renews, or continues credit.

D. Customer: Any person with a covered account with a creditor.

E. Identifying information: 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:

1. name
2. address
3. telephone number
4. social security number

5. date of birth
6. government issued driver's license or identification number
7. alien registration number
8. government passport number
9. employer or taxpayer identification number
10. unique electronic identification number
11. computer's Internet Protocol address or routing code

F. Identity Theft: An attempted or committed fraud using the identifying information another person without permission.

G. Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

II. Identification of Red Flags: In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The following are relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

A. Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the customer

provides (e.g., inconsistent birth dates);

2. Identifying information presented that is inconsistent with other sources of information (i.e., an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (i.e., an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (e.g., very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the College that a customer is not receiving mail sent by the College;
6. Notice to the College that an account has unauthorized activity;
7. Breach in the College's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

1. Notice to the College from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

III. Detecting Red Flags

A. Veterans' deferments of tuition payments

1. New Accounts: In order to detect any of the Red Flags identified within Procedures

Section II associated with the opening of a new account, appropriate College employees will take the following steps to obtain and verify the identity of the person opening the account:

- a. Require certain identifying information such as name, date of birth, residential or business address, driver's license, or other identification;
 - b. Verify the student's identity (e.g., review a driver's license or other identification card);
 - c. Independently contact the student.
2. Existing Accounts: In order to detect any of the Red Flags identified within Procedures Section II for an existing account, appropriate College employees will take the following steps to monitor transactions with an account:
- a. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
 - b. Verify the validity of requests to change billing addresses; and
 - c. Verify changes in banking information given for billing and payment purposes.
- B. Consumer Reports. In order to detect any of the red flags identified within Procedures Section II for a prospective employee for which a consumer credit report is required, appropriate College employees will take the following steps to assist in identifying address discrepancies:
1. Require written verification from any applicant that the address provided by the applicant is accurate at the request for the credit report is made to the consumer reporting agency.
 2. In the event that notice of an address discrepancy is received, verify the credit report pertains to the prospective employee for whom the requested report was made, and report to the consumer reporting agency an address for the prospective employee that the College has reasonably confirmed is accurate.
- C. Tuition installment payment plan (TIP)
1. Students must contact outside service provider and provide personally identifying information to them. (For more information, see Procedures Section VII. Oversight of Service Provider Arrangements).

IV. Responding to Red Flags and Mitigating Identity Theft: In the event of the detection of an identified Red Flag, a College employee shall take all appropriate steps to respond and mitigate the identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to (as appropriate):

- A. Notify their supervisor of the alleged Red Flag detection;
- B. Continue to monitor the account for evidence of identity theft;

- C. Contact the student/employee;
 - D. Change any passwords or other security devices that permit access to accounts;
 - E. Not open a new account;
 - F. Close an existing account;
 - G. Reopen an account with a new number;
 - H. Notify law enforcement; or
 - I. Determine that no response is warranted under the particular circumstances.
- V. Staff Training and Reporting: College employees responsible for implementing the Program shall be trained under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.
- A. Once an employee becomes aware of an identity theft incident, the employee is expected to notify their supervisor or other appropriate administrator of the improper activity in accordance with Procedures Section I of College Policy 6Hx28: 1-10 Policy Against Improper Activities; Whistleblower Protection.
 - B. At least annually or as otherwise requested by the Program Administrator, the Financial Information Security Plan Committee shall report to the Program Administrator through the College Operations Council on compliance with this Program. The report should address such issues as policy and procedures effectiveness in addressing the risk of identity theft in connection with covered accounts, service provider arrangements, and significant incidents involving identity theft and management's response, and recommendations for changes to the Program. For more information, see Procedures Section VI. Program Administrator Responsibilities.

VI. Program Administrator Responsibilities

- A. The Program Administrator is responsible for developing, implementing, and updating the Program throughout the College system. The Program Administrator will be responsible for:
 - 1. ensuring appropriate training of College employees on the Program;
 - 2. reviewing any employee reports regarding the detection of Red Flags; and
 - 3. the steps for identifying, preventing, and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.
- B. The Program Administrator will periodically review the Program to determine if changes are needed in identity theft risks and/or technological changes. As part of the review, the Program Administrator will consider:
 - 1. the College's experiences with identity theft;

2. changes in identity theft methods;
3. changes in identity theft detection, mitigation, and prevention methods;
4. changes in types of accounts the College maintains;
5. changes in the College's business arrangements with other entities; and
6. any changes in legal requirements in the area of identity theft.

After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted.

- C. The Program Administrator shall confer with all appropriate College personnel, Councils, and committees as necessary and appropriate to ensure compliance with the Program. The Program Administrator shall annually report to the College President on the effectiveness of the Program along with any recommended changes for approval.
- VII. Oversight of Service Provider Arrangements. In the event the College engages a service provider to perform an activity in connection with one or more accounts, the College will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:
- A. Require, by contract, that service providers have such policies and procedures in place; and
 - B. Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator.
 - C. In addition, the College will require all persons with any specific questions regarding their covered accounts to contact service providers directly.
- VIII. Reporting Violations
- A. Reports of alleged policy and/or procedure violation(s) should be reported to the Office of Information Technology (OIT) at 407-582-5555 or OITServiceDesk@valenciacollege.edu for initial evaluation. Based on the nature and severity of the allegations, OIT will partner with Organizational Development and Human Resources and/or the Office of Student Rights and Responsibilities, as appropriate, if a College inquiry, investigation, or further assistance is needed.
 - B. If it is determined that a violation has occurred and depending on the nature and severity of the offense, violators of this policy and/or its implementing procedures may be subject to additional and appropriate College action, including but not limited to, College disciplinary action; denial of College technology access and/or College property; and/or criminal prosecution under applicable laws, rules, and regulations. For more information, see College Policies 6Hx28: 3E-08 Disciplinary Action and 6Hx28: 8-03 Student Code of Conduct.
-

Procedure History: Adopted 9-11-25

Related Documents/Procedures:

Date of Last Procedure Review: 09-11-2025