Jamestown Community College
Policies and Procedures

Policy Title	**Identity Theft Protection Program**	**Policy Number**	**305**
Section	**Financial Affairs and Development**	**Approval Date**	**8/1/2009**
Subsection	**General Financial Policies**	**Effective Date**	**8/1/2009**
Responsible Office	**Information Technology**	**Review Date**	**6/24/2019**

1.0 Purpose

1.1 Jamestown Community College developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the College's operations and account systems, and the nature and scope of the College's activities, the Jamestown Community College Board of Trustees determined that this Program was appropriate for the College, and therefore approved this Program on July 21, 2009.

2.0 Policy

2.1 It is the policy of Jamestown Community College (JCC) to establish an Identity Theft Prevention Program, tailored to its size, complexity and the nature of its operation, consistent with the Red Flags Rule.

2.2 An Identity Theft Program must contain reasonable policies and procedures to:

- Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from Identity Theft.

3.0 Procedures

3.1 Identification of Red Flags. In order to identify relevant Red Flags, the College 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. The College identifies the following Red Flags in each of the listed categories:

3.1.1 Notifications and Warnings from Credit Reporting Agencies Red Flags.

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on an applicant;
- Notice or report from a credit agency of an active duty alert for an applicant;
- Receipt of a notice of address discrepancy in response to a credit report request; and
- Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

3.1.2 Suspicious Documents Red Flags.

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing student information; and
- Application for service that appears to have been altered or forged.

3.1.3 Suspicious Personal Identifying Information Red Flags.

- Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another student;
- An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personal identifying information on an application when reminded to do so; and
- A person's identifying information is not consistent with the information that is on file for the student.

3.1.4 Suspicious Covered Account Activity or Unusual use of Account Red Flags.

- Change of address for an account followed by a request to change the student's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use;
- Mail sent to the student is repeatedly returned as undeliverable;
- Notice to the College that a student is not receiving mail sent by the College;
- Notice to the College that an account has unauthorized activity;
- Breach in the College's computer system security; and
- Unauthorized access to or use of student account information.

3.1.5 Alerts from Others Red Flags.

- Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

3.2 Detecting Red Flags.

3.2.1 Student Enrollment. In order to detect any of the Red Flags identified above associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

- **Detect**
  - Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
  - Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

3.2.2 Existing Accounts. In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take the following steps to monitor transactions on an account:

- **Detect**
  - Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
  - 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; and
  - Verify changes in banking information given for billing and payment purposes.

3.3 Preventing and Mitigating Identity Theft. In the event College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

3.3.1 Prevent and Mitigate

- Continue to monitor a Covered Account for evidence of Identity Theft;
- Contact the employee, student, or applicant;
- Change any passwords or other security devices that permit access to Covered Accounts;
- Not open a new Covered Account;
- Provide the student with a new student identification number;
- Notify the Program Administrator for determination of the appropriate step(s) to take;
- Notify law enforcement;
- File or assist in filing a Suspicious Activities Report ("SAR"); or
- Determine that no response is warranted under the particular circumstances.

3.3.2 Protect Student Identifying Information. In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student identifying information.

- Ensure that its website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
- Ensure that office computers with access to Covered Account information are password protected;
- Avoid use of social security numbers (See JCC Information Security Policy);
- Ensure computer virus protection is up to date; and

- Require and keep only the kinds of student information that are necessary for College purposes.

3.4 Administration

3.4.1 Oversight. Responsibility for developing, implementing and updating this Program lies with the Information Security Committee ("Committee") for the College. The Committee is headed by a Program Administrator who may be the President of the College or his or her appointee. Two or more other individuals appointed by the President of the College or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for 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.

3.4.2 Staff Training and Reports. College staff responsible for implementing the Program shall be trained either by or 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. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the College's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, College staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

3.4.3 Service Provider Arrangements. In the event the College engages a service provider to perform an activity in connection with one or more Covered 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.

- Require, by contract, that service providers have such policies and procedures in place; and
- Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator or the College employee with primary oversight of the service provider relationship.

3.4.4 Non-disclosure of Specific Practices. For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other JCC employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

3.4.5 Program Updates. The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the College from Identity Theft. In doing so, the Committee will consider the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

4.0 Definitions

4.1 Identity Theft. A fraud committed or attempted using the identifying information of another person without authority.

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

4.3 Covered Account. includes all student accounts or loans that are administered by the College.

4.4 Program Administrator. The individual designated with primary responsibility for oversight of the program.

4.5 Identifying information. Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: 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.

5.0 References

5.1 Federal Trade Commission's Red Flags Rule.

5.2 Section 114 of the Fair and Accurate Credit Transactions Act of 2003.