

	Identity Theft Prevention Policy	
Business Administration	Administrative Policy TBD	Adopted January 2010 Page 1 of 3

1.0 Identity Theft Policy Objectives and Responsibilities

The risk of data loss and identity theft to Columbia Basin College (the “College”), its employees, and students is a significant concern. In response to the Fair and Accurate Credit Transactions Act of 2003 (FACTA) and in accordance with the Federal Trade Commission (FTC), the College will maintain procedures to identify, detect, and respond appropriately to a pattern, practice, or specific activity indicating the possible existence of identity theft (“red flag”) in order to prevent and/or mitigate harm.

2.0 Definitions

2.1 Covered Account means a covered account involves multiple payments or transactions, as well as any other account the College offers or maintains for which there is a foreseeable identity theft risk, most often in payroll, human resources, accounting, admissions, or financial aid functions.

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

2.3 Information Security Committee means the information security committee is a team, including the program administrator, responsible for developing, implementing and updating the identity theft program, as well as reviewing, investigating, and responding to suspicious activity reports.

2.4 Program Administrator means the program administrator is responsible for program administration and updating the policy. The College program administrator is the Senior Vice President for Administration.

2.5 Red Flag means a red flag is a pattern, practice, or specific activity indicating the possible existence of identity theft.

3.0 Identifying Red Flags

Each department should identify relevant red flags and conduct a risk assessment. Possible sources used for identifying red flags include:

3.1 Credit reporting agency warnings of fraud, credit freezes, or inconsistent credit activity.

3.2 Suspicious documents, such as forged, altered, or inauthentic identification cards.

- 3.3 Suspicious personal identifying information, including forged, altered, incomplete, inconsistent, or inauthentic data, presented on applications, drivers' licenses, social security number, phone number, address, or student records.
- 3.4 Suspicious account activity or unusual use of account, including:
 - 3.4.1 Change of address followed by a request to change the account holder's name.
 - 3.4.2 Payments stopped on an otherwise consistently up-to-date account.
 - 3.4.3 Account use inconsistent with prior use.
 - 3.4.4 Mail sent to the account holder repeatedly returned as undeliverable.
 - 3.4.5 Notice to the College that a student is not receiving mail sent by the College.
 - 3.4.6 Notice to the College that an account has unauthorized activity.
 - 3.4.7 Breach in the College's computer system security.
 - 3.4.8 Unauthorized access to or use of student or staff account information.
 - 3.4.9 Unreasonable change requests.
- 3.5 Notice to the College from a customer, a victim of identity theft, a law enforcement authority or other person, of an act or acts of identity theft.

4.0 Confirming Identity

Each department should develop methods for confirming identity when a red flag is identified. Possible methods for confirming identities include:

- 4.1 Verifying the identity of people making transactions by requiring identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license, or student identification card.
- 4.2 Contacting the student or staff member independently.
- 4.3 Verifying changes requested through a separate contact.

5.0 Preventing and Mitigating Identity Theft

Upon detection and depending upon the degree of risk, staff should take one or more of the following steps to prevent and/or mitigate identity theft as appropriate:

- 5.1 Notify the Information Security Committee in writing of the suspicious activity.
- 5.2 Monitor the account for further evidence of identity theft.
- 5.3 Contact the student or staff member who is the proper owner of the account.
- 5.4 Change passwords or other security codes and devices that permit access to the account.
- 5.5 Disallow opening a new account under the same name.
- 5.6 Close the existing account.

- 5.7 Reopen the account with a new number.
- 5.8 Stop attempts to collect payment on the account.
- 5.9 Notify the program administrator for determination of the appropriate step(s) to take.
- 5.10 Notify law enforcement.
- 5.11 Update the program.

6.0 Protecting Student or Staff Identifying Information

In order to further prevent the likelihood of identity theft, the College shall take the following steps to protect customer identifying information:

- 6.1 Post proper signage in staff/student interaction areas where audio privacy may be a concern.
- 6.2 Undertake complete and secure destruction of paper documents and computer files containing student or staff information pursuant to federal and state laws regarding records retention.
- 6.3 Make office computers password protected and provide training on locking computer screens when leaving work stations during the workday.
- 6.4 Keep offices clear of papers containing customer identifying information.
- 6.5 Request only the last four digits of social security numbers (if any).
- 6.6 Maintain computer virus protection is up to date.
- 6.7 Require and keep only the kinds of customer information that are necessary for College purposes.
- 6.8 Require program administrators to work with the identity theft committee to review this policy periodically so that improvements in identity theft detection and prevention can be identified and implemented.
- 6.9 Require service providers engaged by the College to perform their activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.