

Sensitive Information	Document No.	
	Effective Date	5-25-10
	Revision Date	
	Revision No.	1.0
	Page No.	1 of 5
	Approval:	

1.0 Purpose

This policy establishes guidelines for handling sensitive information.

2.0 Revision History

Date	Rev. No.	Change	Ref Section
	1.0	New policy.	

3.0 Persons Affected

- 3.1 All college employees, including student employees, who work with or have access to sensitive information.
- 3.2 All volunteers who work with or have access to sensitive information.
- 3.3 All third party service providers who work with or have access to sensitive information.

4.0 Policy

The policy of Casper College is to ensure the following.

- 4.1 The college complies with the Fair and Accurate Credit Transaction Act.
- 4.2 The college protects sensitive information that it gathers from students, employees, clients, vendors, and third-party service providers.
- 4.3 The college has processes to identify, investigate, report, and mitigate the misuse of sensitive information.
- 4.4 The college has security measures in place to protect sensitive information.
- 4.5 Employees who work with or have access to sensitive information receive training on the Identity Theft Prevention Program.

5.0 Definitions

- 5.1 Sensitive Information. This is personal information that could potentially be misused. Types of sensitive information include, but are not limited to, credit card, payroll, medical, or personal information or tax identification numbers.
- 5.2 Identity Theft. This is fraud committed or attempted using the identifying information of another person without authorization.
- 5.3 Red Flag. This is a pattern, practice, or specific activity that indicates the possible existence of identity theft. The *Identity Theft Prevention Program* manual contains a list of potential red flags.
- 5.4 Identity Theft Prevention Program Manual. This document is a comprehensive guide to identifying and addressing potential misuse of sensitive information. This document is located at in the office of the vice president of administrative services and at www.caspercollege.edu.
- 5.5 Third Party Service Providers. These are individuals or organizations who provide either on-going or intermittent services to the college.
- 5.6 Covered Account. A new or existing account that involves or is designed to permit multiple payments or transactions including student accounts and loans.

6.0 Responsibilities

- 6.1 Employees who work with or have access to sensitive information are responsible for following the guidelines established in this policy and in the *Identity Theft Prevention Program* manual.
- 6.2 Supervisors and department heads are responsible for ensuring employees who work with or have access to sensitive information complete the required training.
- 6.3 Employees who coordinate volunteers are responsible for ensuring volunteers who work with or have access to sensitive information complete the required training.
- 6.4 The vice president of administrative services is responsible for implementing and ensuring compliance of the Identity Theft Prevention Program.

7.0 Procedures

7.1 Employee Training

- 7.1.1 Supervisors or department heads notify employees who work with or have access to sensitive information that they will need to complete identity

theft prevention training prior to the employees having access to sensitive information.

- 7.1.2 The supervisor or department head will provide the employee with information on how to access the training and a date by which the training must be completed.
- 7.1.3 The employee completes the training and provides her supervisor or department head with the certificate of completion.
- 7.1.4 The supervisor submits the certificate of completion to the Human Resources Department to be filed in the employee's personal file. The department head submits the certificate of completion for a faculty employee to the Office of Academic Affairs to be filed in the faculty employee's personal file.

7.2 Volunteer Training

- 7.2.1 Employees who coordinate volunteers notify volunteers who work with or have access to sensitive information that they will need to complete identity theft prevention training prior to the employees or volunteer having access to sensitive information.
- 7.2.2 Employees who coordinate volunteers will provide the volunteers with information on how to access the training and a date by which the training must be completed.
- 7.2.3 The volunteer completes the training and provides the employee that is coordinating the volunteers with the certificate of completion.
- 7.2.4 The employee who is coordinating the volunteers files the certificate of completion in her volunteer file.

7.3 Implementation

7.3.1 Employees

- 7.3.1.1 Employees will secure all sensitive information upon collection and while in use. Employees will treat information that is questionable as to its sensitivity as sensitive information until determined otherwise.
- 7.3.1.2 Employees will investigate all red flags by following the guidelines in the *Identity Theft Prevention Program* manual.

- 7.3.1.3 Employees will report any red flags to their appropriate vice president or the president.
- 7.3.1.4 The president or vice presidents will report the red flag to the vice president of administrative services.
- 7.3.1.5 The vice president of administrative services will determine what action to take upon completion of a red flag investigation.
- 7.3.1.6 Employees will report non-compliance to the Identity Theft Prevention Program to the vice president of administrative services.

7.3.2 Volunteers

- 7.3.2.1 Volunteers will secure all sensitive information upon collection and while in use. Volunteers will treat information that is questionable as to its sensitivity as sensitive information until determined otherwise.
- 7.3.2.2 Volunteers will report any red flags to the Casper College employee with whom they are working.
- 7.3.2.3 The employee will report the red flag to the vice president of administrative services.
- 7.3.2.4 The vice president of administrative services will determine what action to take upon completion of a red flag investigation.

7.3.3 Third Party Service Providers

- 7.3.3.1 Contractors will have policies and procedures in place to address sensitive information that comply with the Fair and Accurate Credit Transaction Act.
- 7.3.3.2 Contractors will contractually agree to review the college's Identity Theft Prevention Program.
- 7.3.3.3 Contractors will report any red flags to the vice president of administrative services or to the college employee with whom the provider has an oversight relationship.

7.4 Review

7.4.1 The vice president of administrative services is required to review the Identity Theft Prevention Program at least once a year and make any necessary changes to the program.

7.5 Reporting

7.5.1 The vice president of administrative services will report to the Board of Trustees at least once a year on the effectiveness of and compliance to the Identity Theft Prevention Program.