CHAPTER:		DATE ADOPTED	NUMBER
ADMINISTRATION	**Red Flags Program**	July 14, 2009 Revised December 14, 2010	221

SYNOPSIS:

1 Policy: This policy establishes a program through which employees working with covered accounts detect and respond to red flags that could indicate identity theft. The policy was written in accordance with the rules and guidelines set forth in 16 CFR Part 681 implementing the identity theft red flags portion of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

2 Purpose: The protection of Confidential and Sensitive Information assets and the resources that support them are critical to the operation of Iowa Central Community College. As information assets are handled they are placed at risk for potential threats of employee errors, malicious or criminal actions, theft, and fraud. Such events could cause Iowa Central to incur a loss of confidentiality or privacy, financial damages, fines, and penalties.

The purpose of this policy is to reduce the risk of a loss or breach of Confidential and Sensitive Information through guidelines designed to detect, prevent, and mitigate loss due to errors or malicious behavior. Iowa Central recognizes that absolute security against all threats is an unrealistic expectation. Therefore, the goals of risk reduction and implementation of this policy are based on:

- An assessment of the Confidential and Sensitive Information handled by Iowa Central.
- The cost of preventative measures designed to detect and prevent errors or malicious behavior.
- The amount of risk that Iowa Central is willing to absorb.

The Identity Theft Prevention Program Procedures are derived through a risk assessment of Iowa Central methods of handling Confidential and Sensitive Information. Determination of appropriate security measures must be a part of all operations and shall undergo periodic evaluation.

3 Scope: These policies apply to owners, executives, management, employees, and service providers of Iowa Central. This includes all parties that may come into contact with Confidential and Sensitive Information, such as, contractors, consultants, temporaries, and personnel of third party affiliates.

Iowa Central will implement and enforce these policies, as well as, design more specific or new guidelines as needed.

4 Terms and Definitions:

Red Flags – Red Flags are patterns, practices, or specific activities involving covered accounts that indicate the possible risk of identity theft.

Covered Account – Both new and existing accounts where a continuing relationship exists between the Iowa Central and the stakeholder are considered “covered accounts.” There are two definitions.

An account that the institution offers or maintains that involves or is designated to permit multiple payments or transactions. Examples include any account that contains confidential and sensitive information.

Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or mitigation risks.

5 Roles and Responsibilities:

a. Board of Directors - The Board is responsible for the Identity Theft Prevention Program. However, it is not feasible for the Board to be directly involved. The Board appoints the President to oversee the design, implementation, and evaluation of the Identity Theft Prevention Program. The President will assemble a team for this program. This team will be led by Identity Theft Prevention Officer(s) to maintain the Identity Theft Prevention Program. A report will be given to the Board at least annually on the state of the Identity Theft

Prevention Program.

b. Employees - All personnel are responsible for adhering to these guidelines, and for reporting any security incidents to the Identity Theft Prevention Officers immediately.

c. Service Providers - The level of responsibility given to service providers for security reasons depends on the scope of their service offering. Each will be responsible according to their *direct* or *indirect* access to information. In either case, service providers will be held accountable for their conduct and agreements must delineate where Iowa Central's liability ends and where the service provider's liability begins.