**STERLING COLLEGE**

**“Red Flag Rules” /Identity Theft Prevention Policy**

**Adopted January 2012**

1. **Background**

Sterling College (the “College”) has established the following policy in compliance with the Red Flag Rules promulgated by the Federal Trade Commission under Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which require certain financial institutions and creditors to develop and implement written programs designed to detect, prevent and mitigate the risk of identity theft in connection with opening or maintaining certain covered accounts.

1. **Definitions**

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

*Red Flags:* Patterns, practices and specific activities that indicate the possible existence of identity theft.

*Covered Accounts:* An account that the College offers or maintains, primarily for personal, family or household purposes, that involves multiple payments or transactions, and any other account that the College offers or maintains for which there is a reasonably foreseeable risk to account holders or to the College’s financial soundness from identity theft. After conducting a risk assessment to determine whether it offers or maintains any covered accounts, the College has determined that the following accounts may constitute covered accounts:

 Student tuition accounts with a payment plan

 Perkins loans

 Student Account Records

* Admission Records
* Registration Records
* Registrar Records
* Financial Aid Records
* Health Service Records

*Service Provider:* A person or entity which provides services directly to the College in connection with one or more covered accounts. Service providers of the College relating to this program include the College’s providers of student and employee health insurance, third-party retirement and other benefits administrators, financial institutions that administer the College’s tuition payment plan programs, governmental and private student loan providers, electronic billing and payment partners, and collections agencies.

1. **Identifying Red Flags**

The College has considered the following factors in identifying Red Flags for covered accounts:

 The types of covered accounts which the College offers and/or maintains

 The methods the College uses to open accounts

 The methods the College allows to access its covered accounts

 Any previous problems with identity theft involving covered accounts opened or maintained by the College

The following should be considered relevant Red Flags:

 Alerts, notifications, or other warnings received from consumer reporting agencies, service providers, and fraud detection services.

 The presentation of suspicious documents, such as a photo ID not appearing to be authentic or not matching the appearance of the person presenting it.

 The presentation of suspicious personal identifying information, including address discrepancies.

 The unusual use of, or other suspicious activity related to a covered account.

 Notice from customers, students, victims of identity theft, law enforcement, or other persons regarding possible identity theft in connection with covered accounts.

1. **Detection of Relevant Red Flags**

College employees with access to one or more covered accounts shall be aware of the Red Flags set forth in Section III and shall take precautions as circumstances warrant to detect Red Flags, such as verifying the identity of customers/students opening a covered account; and authenticating customers/students, monitoring transactions, and verifying related data in the case of existing covered accounts. Information Services employs additional hardware/software to detect suspicious or unusual network activity.

1. **Response**

Procedures for responding to Red Flags:

1. Any staff member of the College who detects a Red Flag shall report the detection of the Red Flag to his/her department head.

2. The department head will investigate the detection of a Red Flag and will perform an initial risk assessment of the particular Red Flag.

3. Upon completion of a risk assessment, the department head will respond to the detection of the Red Flag as he/she deems appropriate. Suitable responses include but are not limited to: notifying the covered account holder, requiring additional information about the covered account or covered account holder, changing passwords or other security codes, denying access to or closing the covered account, contacting the College’s Vice President/CFO and notifying law enforcement and/or other state agencies. The department head may also determine that no response is warranted under the particular circumstances.

4. Additionally, the department head shall report any Red Flags and the response taken to the Vice President /CFO.

1. **Oversight**

The Vice President/CFO has been designated as the appropriate person to oversee this policy on an ongoing basis. He may designate an appropriate person to develop, implement and administer this policy. Any questions regarding this policy should be directed to the Vice President/CFO.

Outside Service Providers: The College will require all of its service providers that provide services directly to the College in connection with covered accounts to comply with the College’s Red Flags policy or to adopt reasonable written policies and procedures designed to detect, prevent, and mitigate the risk of identity theft in accordance with the Red Flag Rules, and to provide the College with timely written notice of Red Flags relating to such covered accounts. The College will inform service providers of this policy.

Each department will assure that third party service providers are required to maintain appropriate safeguards for nonpublic information to which they have access. Contracts with service providers, who within their contracts have access to Sterling College non-public customer information, shall include the following provisions as appropriate:

* Explicit acknowledgment that the contract allows the contract partner access to confidential information;
* Specific definition of the confidential information being provided;
* Stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
* Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
* Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
* Guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;
* Provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
* Stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
* Stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Sterling College to immediately terminate the contract without penalty;
* Provision allowing auditing of the contract partners' compliance with the contract safeguard requirements;
* Provision ensuring that the contract's protective requirements shall survive any termination agreement.

Training

The Vice President/CFO shall designate an appropriate person to coordinate the training of staff, as necessary, to effectively implement this policy. College employees with access to one or more covered accounts shall be made aware of this policy and any material amendments to this policy.

Reassessment of Plan

This policy will be reviewed periodically and adjusted as needed to reflect changes in risks to customers based on factors such as:

 The experiences of the College with identify theft;

 Changes in methods of identity theft;

 Changes in methods to detect, prevent, and mitigate identity theft;

 Changes in the types of accounts that the College offers or maintains; and

 Changes in the business arrangements of the College, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Annual Report

On an annual basis, each department head shall prepare a report regarding compliance with this policy to be reviewed by the Vice President/CFO. The report shall address and evaluate issues such as:

 The effectiveness of this policy in addressing the risks of identity theft in connection with covered accounts;

 Service provider arrangements, as applicable;

 Significant incidents involving identity theft and the department’s response; and

 Recommendations for material changes to this policy.