The College’s Program shall include reasonable procedures and processes to:

1. Identify relevant red flags for covered accounts and incorporate those red flags into the program.
2. Detect red flags that have been incorporated in the program.
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
4. Ensure the program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft.

The College has identified the following types of accounts and information:

1. Student information including FERPA covered restricted information
2. Deferment of tuition payments
3. Electronic fund transfer account numbers and other bank related information
4. Credit and Debit card information
5. Short term student emergency loans
6. Financial aid refunds
7. Social security numbers
8. Personnel files

Administration of the Program

1. The Vice President for Administrative Services shall be responsible for the development, implementation, oversight and continued administration of the Program.
2. Appropriate staff will be trained, as necessary, to effectively implement and monitor the program.
3. Appropriate and effective oversight of any external service provider shall be incorporated within the program.

Categories of Red Flags

Examples of red flags included in the program are as follows:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.
2. The presentation of suspicious documents or personal identifying information.
3. The unusual use of, or other suspicious activity, related to a covered account.
4. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
5. Notices of address discrepancies.
6. Recent increases in the volume of new inquiries or patterns of activity that are inconsistent with prior history.

Identification of Red Flags

The program shall address the detection of red flags in connection with the opening of covered accounts and existing covered accounts by:

1. Obtaining identifying information about, and verifying the identity of a person opening a covered account.
2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.
3. Making every effort to limit access to information to only those with legitimate “need to know” basis.
4. All files for employees, students and others shall be in locked filing cabinets and offices shall be locked when not occupied.
5. All documents containing protected information shall be shredded and disposed of in a secure way.

Response to detected Red Flags

Appropriate responses to detected red flags to prevent and mitigate identity theft should be taken. The response shall be commensurate with the degree of risk posed.

Appropriate responses may include but are not limited to:

1. Monitor a covered account for evidence of identity theft.
2. Contact the customer.
3. Change any passwords, security codes or other security devices that permit access to a covered account.
4. Reopen a covered account with a new account number.
5. Close or place a hold on an existing covered account.
6. Notify appropriate college officials or law enforcement.
7. Determine no response is warranted under the particular circumstances.
8. Notify appropriate college officials or law enforcement.
9. Determine no response is warranted under the particular circumstances.

The program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the College from identity theft.

Oversight of the program shall include

1. Assignment of specific responsibility for the implementation of the program.
2. Review of any reports that may be developed by staff regarding compliance.
3. Approval of material changes to the policy or procedure related to the procedures to address changing risks of identity theft.
4. Taking steps to ensure the activity of any third party service provider engaged by the College has reasonable policies and procedures in place to detect, prevent, and mitigate the risk of identity theft in conjunction with the College’s covered accounts.