**BBCC Administrative Process**
**AP# 8300 *Identity Theft Prevention Program*** **Implementing Board Policy: BP8300**
**Effective Date: 7/10/2020** **Responsible Department: Finance & Administration**

1.0 PURPOSE

Identification of Red Flags to prevent identity theft

2.0 SCOPE

a. Oversight

Responsibility for developing, implementing and updating this Program lies with the Executive Director of Business Services. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft.

b. Staff Training and Reports

College staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

c. Program Updates

The Administrator will periodically review and update this Program to reflect changes in risks to students/staff and the soundness of the College from Identity Theft. In doing so, the Administrator will consider the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Administrator will update the Program.

3.0 DEFINITIONS

3.1 Red Flags Rules Definitions Used in this Program

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

Red Flag - a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Covered Account - includes all accounts or loans that are administered by the College including, but not limited to:

a. Student Tuition Easy Payment Plan

b. Student Financial Aid
c. Perkin Loans
d. Human Resources
e. Payroll
f. Admissions

Program Administrator - the individual designated with primary responsibility for oversight of the program. See Section 2.0 above.

Identifying information - any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address or routing code.

## 4.0 PROCESS

### 4.1 Identification of Red Flags

A. Suspicious Documents

<u>Red Flags</u>

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information; and
4. Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

<u>Red Flags</u>

1. Identifying information presented that is inconsistent with other information the person provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address in student records);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5. Social security number presented that is the same as one already in the system;
6. A person fails to provide complete personal identifying information on an application when reminded to do so; and
7. A person's identifying information is not consistent with the information that is on file for the person.

C. Suspicious Covered Account Activity or Unusual Use of Account

<u>Red Flags</u>

1. Change of address for an account followed by a request to change the person's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the College that an account has unauthorized activity;
6. Breach in the College's computer system security; and
7. Unauthorized access to or use of student account information.

D. Alerts from Others

<u>Red Flag</u>

1. Notice to the College from an Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

4.2 Detecting Red Flags

In order to detect any of the Red Flags identified above, College personnel will take the following steps to monitor transactions on a covered account:

A. New Accounts
<u>Detect</u>

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the identity at time of issuance of identification card (review of driver's license or other government-issued photo identification or original passport or visa for international students), to the extent allowed by law.

B. Existing Accounts

<u>Detect</u>

1. Verify the identification of the person requesting information (in person, via telephone, via facsimile, via email);

2. Verify the validity of requests to change billing addresses by mail or email and provide a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

4.3 Preventing and Mitigating Identity Theft

In the event College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Contact the student or applicant;
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Not open a new Covered Account;
5. Provide the person with a new identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report (“SAR”); or
9. Determine that no response is warranted under the particular circumstances.

Protect Student Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing personal account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to Covered Account information are password protected;
4. Avoid use of social security numbers;
5. Only release student information to the student in compliance of FERPA laws, unless a consent form has been completed by the student;
6. Ensure computer virus protection is up to date;
7. College will never send a request for identifying information by email; and
8. Require and keep only the kinds of personal information that are necessary for College purposes.

**Approving Body: Shared Governance Council**
***Document History (8/4/09, 7/10/2020)***