IV:07:11 IDENTITY THEFT PREVENTION POLICY

SECTION 1: BACKGROUND

The risk to Volunteer State Community College ("College") its faculty, staff, students and other applicable constituents from data loss and identity theft is of significant concern and the College will make reasonable efforts to detect, prevent, and mitigate identity theft.

SECTION 2: PURPOSE

Adoption of this policy and program is an effort to detect, prevent and mitigate identity theft, and to help protect the College from damages related to the loss or misuse of identifying information due to identity theft.

Under this policy the program will:

1. Identify patterns, practices or specific activities ("red flags") that could indicate the existence of identity theft with regard to new or existing covered accounts (defined below in Section 3);
2. Detect red flags that are incorporated in the program;
3. Respond appropriately to any red flags that are detected under this program to prevent and mitigate identity theft;
4. Ensure periodic updating of the program, including reviewing covered accounts and the identified red flags that are part of this program; and,
5. Promote compliance with state and federal laws and regulations regarding identity theft protection.

The program shall, as appropriate, incorporate existing College policies and guidelines such as anti-fraud programs and information security programs that control reasonably foreseeable risks

SECTION 3: DEFINITIONS

"Covered account" includes:

1. Any account that involves or is designated to permit multiple payments or transactions; or
2. Any other account maintained by the College for which there is a reasonably foreseeable risk of identity theft to students, faculty, staff or other applicable constituents, or for which there is a reasonably foreseeable risk to the safety or soundness of the College from identity theft, including financial, operational, compliance, reputation or litigation risks.

"Identifying information" is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: 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 Internet Protocol address or routing code, credit card number or other credit card information.

"Identity theft" means a fraud committed or attempted using the identifying information of another person without authority.

"Red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

SECTION 4: IDENTIFICATION OF RED FLAGS

The following examples of red flags are potential indicators of fraud or identity theft. The risk factors for identifying relevant red flags include the types of covered accounts offered or maintained; the methods provided to open or access covered accounts; and, previous experience with identity theft. Any time a red flag or a situation closely resembling a red flag is apparent, it should be investigated for verification.

Alerts, notifications or warnings from a credit or consumer reporting agency

Examples of these red flags include the following:

1. A report of fraud or active duty alert in a credit or consumer report;
2. A notice of credit freeze from a credit or consumer reporting agency in response to a request for a credit or consumer report;
3. A notice of address discrepancy in response to a credit or consumer report request; and,
4. A credit or consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant such as:

    - A recent and significant increase in the volume of inquiries;
    - An unusual number of recently established credit relationships;
    - A material change in the use of credit, especially with respect to recently established credit relationships; or,
    - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious documents

Examples of these red flags include the following:

1. Documents provided for identification that appear to have been altered, forged or are inauthentic.
2. The photograph or physical description on the identification document is not consistent with the appearance of the individual presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or individual presenting the identification.
4. Other information on the identification is not consistent with readily accessible

information that is on file with the College.

5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious personal identifying information

Examples of these red flags include the following:

1. Personal identifying information provided is inconsistent when compared against other sources of information used by the College. For example: The social security number has not been issued or is listed on the Social Security Administration's Death Master File.
2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by that individual.
3. Personal identifying information provided is associated with known fraudulent activity. For example:
   - The address on an application is the same as the address provided on a fraudulent application; or,
   - The phone number on an application is the same as the number provided on a fraudulent application.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity.
5. The social security number provided is the same as that submitted by another person.
6. The address or telephone number provided is the same as or similar to the address or telephone number submitted by that of another person.
7. The individual opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
8. Personal identifying information provided is not consistent with personal identifying information that is on file with the College.
9. When establishing security questions (mother's maiden name, pet's name, etc.), the person opening that covered account cannot provide authenticating information beyond that which generally would be readily accessible.

Unusual use of, or suspicious activity related to, the covered account

Examples of these red flags include the following:

1. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: Nonpayment when there is no history of late or missed payments;
2. Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.
3. The College is notified that the individual is not receiving paper account statements.
4. The College is notified of unauthorized charges or transactions in connection with an individual's covered account.
5. The College receives notice from customers, victims of identity theft, law

enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the College.
6. The College is notified by an employee or student, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
7. A breach in the College's computer security system.

SECTION 5: DETECTING RED FLAGS

Student enrollment

In order to detect red flags associated with the enrollment of a student, the College will take the following steps to obtain and verify the identity of the individual opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and.
2. Verify the student's identity at the time of issuance of the student identification card through review of driver's license or other government-issued photo identification.

Existing accounts

In order to detect red flags associated with an existing account, the College will take the following steps to monitor transactions on an account:

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

SECTION 6: RESPONDING TO RED FLAGS

The College must act quickly with consideration of the risk posed by a red flag or potential red flag, if detected.

The College should gather all related documentation in a timely manner, write a description of the situation and present this information to the Vice President of Business and Finance for determination.

The Vice President of Business and Finance (see Section 8) will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

The College may take the following steps as is deemed appropriate:

1. Continue to monitor the covered account for evidence of identity theft;
2. Change any passwords or other security devices that permit access to covered accounts;

3. Close and reopen the account;
4. Determine not to open a new covered account;
5. Provide the student or employee with a new identification number;
6. Notify law enforcement;
7. Determine that no response is warranted under the particular circumstances.
8. Cancel the transaction.

SECTION 7: PROTECTING PERSONAL INFORMATION

In order to prevent the likelihood of identity theft occurring with respect to covered accounts, the College may take the following steps with respect to its internal operating procedures:

1. Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with covered account information when not in use.
2. Lock storage rooms containing documents with covered account information and record retention areas at the end of each workday or when unsupervised.
3. Clear desks, workstations, work areas, printers and fax machines, and common shared work areas of all documents containing covered account information when not in use.
4. Documents or computer files containing covered account information will be destroyed in a secure manner. College records may only be destroyed in accordance with the Board's records retention guideline, TBR Guideline G-070 Disposal of Records.
5. Ensure that office computers with access to covered account information are password protected.
6. Ensure that computer virus protection software is up to date.
7. Avoid the use of social security numbers.

College personnel are encouraged to use common sense judgment in securing covered account information to the proper extent. Furthermore, this section should be read in conjunction with the Family Education Rights and Privacy Act (“FERPA”), the Tennessee Public Records Act, and other applicable laws and policies. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor. The Office of the General Counsel at TBR may be contacted for advice.

SECTION 8: PROGRAM ADMINISTRATION

Oversight of the Program

Responsibility for developing, implementing and updating this program lies with the College’s Vice President Business and Finance. The Vice President Business and Finance is responsible for program administration, ensuring appropriate training of the College’s staff on the program, reviewing any reports regarding the detection of red flags on the identified covered accounts and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the program.

Updating the Program

This program will be periodically reviewed and updated to reflect changes in risks to students and employees and the soundness of the College from identity theft related to the noted covered accounts. At least once per fiscal year, the Vice President Business and Finance will consider the College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the College's business arrangements with other entities, as they relate to this program. After considering these factors, the Vice President Business and Finance will determine whether changes to the program, including the listing of red flags, are warranted. If warranted, the program will be updated.

Staff Training

The College staff responsible for implementing the program shall be trained either by or under the direction of the Vice President Business and Finance in the detection of red flags, and the responsive steps to be taken when a red flag is detected.

Overview of service provider arrangements
It is the responsibility of the College to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designated to detect, prevent, and mitigate the risk of identity theft. In the event the College engages a service provider to perform an activity in connection with one or more covered accounts, the College will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

1. Require, by contract, that service providers have such policies and procedures in place; or,
2. Require, by contract, that service providers review the College's program and agree to report any red flags to the Vice President of Business and Finance.

Specific language for inclusion in contracts can be found in the College's Agreement/Contract Policy (I:01:02) or in TBR Guideline G-030 Contracts and Agreements.

A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

VSCC Source: President's Cabinet, January 31, 2011