11:04:01:00 Identity Theft Detection and Prevention

Purpose:

The purpose of this policy is to establish an Identity Theft Detection and Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall:

1. Identify relevant red flags for covered accounts DSCC offers or maintains and incorporate those red flags into the program.
2. Detect red flags that occur in daily operations by incorporating detection procedures.
3. Prevent and mitigate identity theft by responding appropriately to detected red flags.
4. Ensure the Program is updated periodically to reflect changes in risks to Students and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Scope:

This policy applies to employees, contractors, consultants, temporaries, and other workers at Dyersburg State Community College (DSCC).

Policy:

Identity Theft Detection and Prevention Program
Program Adoption
DSCC developed this Identity Theft Detection and Prevention Program (“Program”) pursuant to Tennessee Board of Regents (TBR) Policy 4:01:05:60 and the Federal Trade Commission’s Red Flags Rule (“Rule”), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This program was developed with oversight and approval of the President, the President’s staff and Administrative Council. After consideration of the size of the College’s operations, account systems, and the nature and scope of the College’s activities, this Program was deemed appropriate for DSCC and therefore approved this Program on September 18, 2009. The College also has an Information Security Policy which addresses protecting personal information which was

approved on September 18, 2009 which should be used in conjunction with the Identity Theft Detection and Prevention Program.

Covered Accounts

DSCC has identified that student accounts are considered a covered account. Three type of activities related to the student account make it a covered account. These are:

1. Refund of credit balances
2. Deferment of tuition payments
3. Participation in the student loan process

Identification of Relevant Red Flags

The Program considers the following risk factors in identifying relevant red flags for covered accounts:

1. The type of covered account as noted above.
2. Method of opening new student accounts based on documents received.
3. Method of providing access to existing student accounts in varying situations.
4. The College's previous history of identity theft.

The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification.
3. A request to mail something, such as a check, to an address not listed on file.
4. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
5. Unusual account activity.

Detection of Red Flags

Mitigating Controls

DSCC has mitigating controls to minimize the ability of a person to commit fraud at the college. Suspicious documents or suspicious personally identifying information presented or obtained during the execution of these controls would be a red flag.

1. Mitigating controls related to opening a new covered account are:
   a. Acceptance to the College and enrollment in classes requires the following information:
   i. Admission application with personally identifying information
   ii. High school transcript or GED score and, if applicable, transcripts from other postsecondary institutions or training agencies including the United States armed forces
   iii. Official ACT or SAT scores and, if applicable, CLEP, AP, DANTES and CPS scores
   iv. Immunization history

b. Eligibility for Financial Aid has the following requirements:
i. Official ISIR must be received from the Department of Education.
ii. Federal matching rules are applied by the Department of Education before the ISIR is submitted to the institution noting any discrepancies. Financial Aid collects documents as necessary to resolve conflicts. Unresolved conflicts are reported to the Inspector General.
iii. When ISIRs are loaded into the DSCC Banner system, matching compares ISIR data to data submitted on the admissions application and conflicts are resolved.
c. Upon receipt of the ACH Payment Enrollment Authorization Form, the Business Office staff verifies that the SS or Student ID # provided matches the named signature on the form. Once the information is keyed into the system, an email notification is sent to the student's MyDSCC email account informing the student that the information provided on the form has been entered.
d. Student's identity is verified at the time of issuance of the student identification card through review of driver's license or other government-issued photo identification.

2. Mitigating controls related to accessing a covered account are:
   a. Disbursements obtained in person require picture identification.
   b. Disbursements obtained by mail can only be mailed to an address on file.
   c. Disbursements made via direct deposit are made to the account number provided by the student. E-mail notification is sent to the student's MyDSCC email account when a refund has been deposited into the account number on file for the student.
   d. Mailing address changes are made by the student in a secure system.
   e. Password changes are made with the following stipulations:
   i. In person, the student must provide their student ID or other government-issued photo identification.
   ii. Via telephone, the student must answer a series of personally identifiable questions.
   iii. Via the software provided on the web site, the student must answer a series of personally identifiable questions.
3. Refunds of credit balances for currently enrolled students are initiated by the college as adequate student attendance is verified by the faculty. The refund may be mailed to an address on file or deposited into the bank account designated on the ACH Payment Enrollment Authorization Form. Students receiving refunds via a direct deposit are sent an e-mail detailing the amount of the refund.
4. Students who choose to enroll themselves in the deferred payment plan use a secure system.

Red Flags considered to be most likely to occur at DSCC include:

- Suspicious documents are presented.
  o Student presents Picture ID which does not appear to be authentic or not matching the appearance of the student presenting it.
  o Information on document is inconsistent with other information available about the student. This includes ISIR not matching admissions application information.
  o Document appears to be forged or gives the appearance of having been destroyed and reassembled.
- Unusual account activity
  o Student calls indicating they received an e-mail about a refund but the money has not been deposited in their

account.
o Student calls indicating they have not received their billing statement.
- Additional information and examples can be found in TBR policy 4:01:05:60.

Response to detected red flags

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag.
2. Continue to monitor the covered account for evidence of identity theft.
3. Contact the student.
4. Change any passwords, security codes or other security devices that permit access to a covered account.
5. Close and reopen the account.
6. Determine not to open a new covered account.
7. Provide the student with a new student identification number.
8. Notify law enforcement.
9. Contact the Office of the Inspector General if conflicting information on Financial Aid application can't be resolved.
10. Determine no response is warranted under the particular circumstances.
11. Cancel the transaction.

Any detected red flags should be reported to the Red Flag Program Administrator.

Oversight of the Program

Responsibility for developing and updating this Program lies with the Vice President for Technology who has been designated as the Program Administrator. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of College's staff on the Program, for reviewing any staff reports regarding the detection of Red Flags 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 determine whether all aspects of the program are up to date and applicable. At least once per year in March, the Program Administrator 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. 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 Program Administrator will update the Program which would then be submitted for approval to the President, the President's staff and the Administrative Council.

Staff Training

DSCC 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.

Oversight of Service Provider Arrangements
DSCC shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. DSCC has contracts obtained through and negotiated by TBR with Touchnet and collection agencies which require the service providers to adhere to the Red Flags Rule.

Compliance:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or suspension.

Definitions:

Identify theft – Attempted or committed fraud using the identifying information of another person without authority.
Covered account – An account that a creditor offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.
Red flag – A pattern, practice or specific activity that indicates the possible existence of identity theft.

Revision History:

Policy written September, 2009. Policy revised June 2013; approved by Administrative Council on 06/26/13. Policy revised October 2017; approved by Administrative Council on 10/27/17.