1. **Policy Statement**

   Texas A&M International University ("University") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags 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 chancellor as designated by the board of Regents. After consideration of the size and complexity of the University's operations and account systems, and the nature and scope of the University's activities, the chancellor determined that this program was appropriate for the University, and approved this Program on May 1, 2009.

2. **Definitions**

   Identity Theft: a 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: a consumer account designed to permit multiple payments or transactions, and any other account for which there is a reasonably foreseeable risk from identity theft. This generally includes all student accounts or loans that are administered by the University.
   Program Administrator: the individual designated with primary responsibility for oversight of the program.
   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, University issued identification number, computer's internet protocol address, or routing code.

3. **Requirements of the Red Flags Rule**

   Under the red flags rule, the University is required to establish an Identity Theft Prevention Program tailored to its size, complexity and the nature of its operation. Each program must contain reasonable procedures to:

   a. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program;
   b. Detect red flags that have been incorporated into the program;
   c. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
   d. Ensure the program is updated periodically to reflect changes in risks to customers including students or to the safety and soundness of the University from identity theft.

4. Identifications of Red Flags

In order to identify relevant red flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. The University identifies the following red flags in each of the listed categories:

a. **Suspicious Documents**
   i. Identification document or card that appears to be forged, altered or inauthentic;
   ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
   iii. Other document with information that is not consistent with existing customer/student information; and
   iv. Application for services that appears to have been altered or forged.

b. **Suspicious Personal Identifying Information**
   i. Identifying information presented that is inconsistent with other information the customer/student provides (example: inconsistent birth dates);
   ii. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a financial aid application);
   iii. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
   iv. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
   v. Social security number presented that is the same as one given by another customer/student;
   vi. A person fails to provide complete personal identifying information on a required form when reminded to do so; and
   vii. A person's identifying information is not consistent with the information that is on file for the customer/student.

c. **Suspicious Covered Account Activity or Unusual Use of Account**
   i. Change of address for an account followed by a request to change the student's name;
   ii. Payments stop on an otherwise consistently up-to-date account;
   iii. Mail sent to the student is repeatedly returned as undeliverable;
   iv. Notice to the University that a customer/student is not receiving mail sent by the University;
   v. Notice to the University that an account has unauthorized activity;
   vi. Breach in the University's computer system security; and
   vii. Unauthorized access to or use of customer/student account information.

       d. Alerts from Others
           i. Notice to the University from a customer/student, identity theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft.

5. Detecting Red Flags

       a. Student Enrollment
       In order to detect any of the red flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening this account:
           i. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
           ii. Verify the student's identity at the time of issuance of student identification card (review of driver's license or other government-issued photo id, or other personally identifying information for dual credit high school students who do not have a photo id).

       b. Existing Accounts
       In order to detect any of the red flags identified above for an existing covered account, University personnel will take the following steps to monitor transactions on an account:
           i. Verify the identification of students if they request information in person, by telephone, facsimile or email;
           ii. Verify the validity of request to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes.

       c. Background Report Requests
       In order to detect any of the red flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:
           i. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the background check is made to the police department; and
           ii. In the event that notice of an address discrepancy is received, verify that the background report pertains to the applicant for whom the requested report was made.

6. Preventing and Mitigating Identity Theft

In the event University 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:

a. **Prevent and Mitigate**
    i. Flag the covered account so that it can continue to be monitored for evidence of identity theft;
    ii. Contact the customer/student or applicant (for which a background check was run);
    iii. Change any passwords or other security devices that permit access to covered accounts;
    iv. Provide the student with a new student identification number;
    v. Notify the program administrator for determination of the appropriate step(s) to take;
    vi. Notify law enforcement;
    vii. File or assist in filing a Suspicious Activities Report; or
    viii. Determine that no response is warranted under the particular circumstances.

b. **Protect Student Identifying Information**
In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the University will take the following steps with respect to its internal operating procedures to protect student identifying information:
    i. Ensure that its website is secure or provide clear notice that the website is not secure;
    ii. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
    iii. Ensure that office computers with access to covered account information are password protected;
    iv. Avoid use of social security numbers;
    v. Ensure computer virus protection is up to date; and
    vi. Require and keep only the customer/student information that is necessary for University purposes.

7. **Responding to Red Flags**

Once potentially fraudulent activity is detected, an employee must:

a. Act quickly as a rapid appropriate response to protect customers and the University from damages and loss;
b. Gather all related documentation and write a description of the situation; and
c. Present this information to the program administrator for determination.
d. The program administrator or his/her designee will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.
e. If the transaction is determined to be fraudulent, the following appropriate actions must be taken:
    i. Canceling the transaction;
    ii. Notifying and cooperating with appropriate law enforcement;

iii. Determining the extent of liability, if any, of the University; and

iv. Notifying the actual customer that fraud has been attempted.

8. **Program Administration**

   a. **Oversight**
   Responsibility for developing, implementing and updating this program lies with an Identity Theft Committee ("Committee") for the University. The committee is headed by a program administrator. At least three other individuals who are appointed by the program administrator and represent admissions, financial aid, information technology, the registrar, the comptroller and student housing comprise the remainder of the committee membership. The program administrator will be responsible for ensuring appropriate training of University staff on the program, for reviewing any staff reports regarding the detection of red flags, steps for preventing and mitigating identity theft, and determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the program.

   b. **Staff Training and Reports**
   University 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. University staff shall be trained, as necessary, to effectively implement the program. University employees are expected to notify the program administrator once they become aware of an incident of identity theft or of the University's failure to comply with this program. At least annually or as otherwise requested by the program administrator, University staff responsible for development, implementation and administration of the program shall report to the program administrator on compliance with this program. The report should address such issues as effectiveness of the procedures in addressing the risk of identity theft in connection with opening and maintenance of covered accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the program.

   c. **Service Provider Arrangements**
   In the event of the University engages a service provider to perform an activity in connection with one or more covered accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable procedures designed to detect, prevent and mitigate the risk of identity theft. The service provider must have such policies and procedures in place and upon review of the University's program, report any red flags to the program administrator or the University employee with primary oversight of the service provider relationship.

   d. **Non-disclosure of Specific Practices**
   For the effectiveness of this identity theft prevention program, knowledge about specific red flag identification, detection, mitigation and prevention practices may need

to be limited to the committee who developed this program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential and should not be shared with other employees or the public, to the extent permitted by law. The program administrator shall inform the committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

e. **Program updates**
The committee will periodically review and update this program to reflect changes in risks to students and the soundness of the University from identity theft. In doing so, the committee will consider the University's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts offered or maintained, and changes in the University's business arrangements with other entities. After considering these factors, the program administrator will determine whether changes to the program, including the list of red flags, are warranted. If warranted, the committee will update the program.

f. **Contact Information**
To report any potential red flag activity go to www.tamiu.edu/reportit and click on the Identity Theft Prevention Form. For questions regarding the Red Flags Rule please contact the Program Administrator at 956-326-2812.