TRINITY INTERNATIONAL UNIVERSITY

TIU POLICY: **Identity Theft Prevention Policy ("Red Flags" Rule)**

TIU POLICY #: **P-106**

STATUS: **Approved, June 2010**
Updated, May 2015

I. PURPOSE:

The "Red Flags" Rule, in effect since January 1, 2008 requires Trinity International University (University) to implement a written Identity Theft Prevention Program ("The Program") designed to detect the warning signs – or "red flags" of identity theft. The Red Flags Rule is enforced by the Federal Trade Commission (FTC). The purpose of this policy is fourfold:

A. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the University's Identity Theft Program, i.e. What are the red flags?;

B. Spell out procedures for detecting red flags;

C. Articulate the University's response when a red flag is detected;

D. Identify how the University's program will be periodically re-evaluated to insure that it is responsive to new risks and the ever-changing threat of identity theft.

II. SCOPE AND DEFINITIONS:

The scope of this policy is a "**covered account**" as defined below.

The University's Identity Theft Program is designed with consideration given to the size, complexity and scope of the University's operations, account systems and activities.

Definitions:

"**Covered Account**" - all student accounts or payment plans that are administered by the University. Additionally, the University's program is designed to consider the identity theft risk to both donors and employees of the University.

"**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: name, address, telephone number, social security number or taxpayer identification number, date of birth, state issued driver's license or identification number, alien registration number, passport number, student identification number, Internet Protocol address, or bank routing codes and account information including credit and debit cards.

"**Identity Theft**" - a "fraud committed or attempted using the identifying information of another person without authority." For example, a person applies for a student loan using another person's social security number.

"**Identity Theft Committee**" - the individuals designated with primary responsibility for oversight of the program.

"**Red Flag**" - a "pattern, practice, or specific activity that indicates the possible existence of identity theft."

III. POLICY:

A. Identification of Red Flags

The following Red Flags have been identified by the University:

1. Suspicious Documents
   a. Identification document or card that appears to be forged, altered or inauthentic;
   b. Identification document or card on which a person's information, photograph or physical description is not consistent with the person presenting the document;
   c. Application or request for services that appears to have been altered or forged.

2. Suspicious Personal Identifying Information
   a. Identifying information presented that is inconsistent with other information provided (e.g. inconsistent birth dates);
   b. Identifying information presented that is the same as information shown on other documents that have been found to be fraudulent;
   c. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
   d. Social security number presented that is the same as one given by another person;
   e. A person failing to provide complete personal identifying information when required to do so.

3. Suspicious Covered Account Activity or Unusual Use of Account
   a. Notice to the University that a person is not receiving mail sent by the University;
   b. Notice to the University that an account has unauthorized activity;
   c. Breach in the University's computer system security; or
   d. Unauthorized access to, or use of, personal account information.

4. Alerts from Others
   a. Notice received that the University is or may be maintaining a fraudulent account.

B. Detecting Red Flags

1. When Establishing New Accounts

In order to detect any of the Red Flags identified above associated with a Covered

Account, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

a. Require certain identifying information such as name, date of birth, academic records, home address or other identification;
b. Record social security numbers directly into the appropriate University's computer system;
c. Assign an account number which shall be unique to that account; and
d. Re-verify the individual's identity at the time of issuing a University identification card (e.g. driver's license or other government-issued photo identification).

2. On Existing Accounts

In order to detect any Red Flags for an existing Covered Account, University personnel will take the following steps:

a. Verify the identification of any individual requesting information (in person, via telephone, via facsimile or via email);
b. Verify the validity of mailed or emailed requests to change account address; and
c. Verify changes in banking information given for billing and payment purposes.

C. Preventing and Mitigating Identity Theft

In order to prevent identity theft the following internal operating procedures will be followed:

1. Maintain security of the University website;

2. Protect access to all University computers with secure passwords;

3. Update computer virus protection on a regular basis;

4. Ensure that access to all Covered Accounts are password protected and limited to authorized personnel;

5. Require that all passwords be changed on a regular basis;

6. Report any unauthorized access to, or breach of, a Covered Account immediately to the Identity Theft Committee;

7. Secure all documents containing a social security number;

8. Mask social security numbers to the extent possible in all data bases;

9. Accept on-line credit card payments through a third party processing service provider;

10. Accept credit card payments over the phone by directly entering the information into the terminal or securing the written information used to manually enter the card data;

11. Include only the last four digits of a credit card, debit card or bank account number in any issued receipt;

12. Ensure complete and secure destruction of paper documents and computer files containing student account or financial information in accordance with the Record Retention Policy; and

13. Require and keep only information necessary for business purposes of the University.

D. Response to Red Flag Detection or Identity Theft

In the event there is a detection of any identified Red Flags, personnel will notify the Identity Theft Committee for determination of the appropriate step(s) to be taken. These steps may include:

1. Contacting the individual(s) being targeted;

2. Continued monitoring of a Covered Account for evidence of identity theft;

3. Changing any passwords or other security devices that permit access to Covered Accounts;

4. If a student, provide the student with a new student identification card;

5. Opting not to open a new Covered Account;

6. Notifying law enforcement; or

7. Determining that no response is warranted under the particular circumstances.

E. Program Administration

1. Oversight
   a. Identity Theft Committee - Responsibility for developing, implementing and updating The Program lies with the Identity Theft Committee (Committee). The Committee will be comprised of representatives from the following areas:
      i. Student Life
      ii. Student Financial Services
      iii. Human Resources
      iv. University Services
      v. Information Technology

2. Responsibility - The Committee will be responsible for:
   a. Incident reporting and response.
   b. Monitoring area compliance with prevention and detection procedures.
   c. Periodic review of the policy in accordance with any statutory changes, experiences with identity theft situations, or best practice changes in the prevention or detection of identity theft methods.

3. Meeting Frequency - The Committee will meet at least quarterly.

4. Reporting - At least annually, the Identity Theft Committee will report to the University Leadership Team (ULT). The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft along with management's response, and recommendations for changes to the Program.

F. Staff Responsibilities

Employees are expected to notify the Committee immediately when they detect a Red Flag, become aware of an incident of identity theft, or become aware of the University's failure to comply with The Program procedures.

Additionally, specific considerations of the University's prevention, detection and reporting include:

1. Admissions:
   a. Establishing new accounts
   b. Changing applicant information
   c. Verifying identity documents for new students

2. Student Services:
   a. Changing student information
   b. Verifying identity prior to issuing a Trinity ID card
   c. Verifying international student documentation

3. Financial Aid:
   a. Verifying documents submitted for financial aid qualification
   b. Responding to requests for information

4. Office of the Registrar:
   a. Changing student information
   b. Responding to requests for student documents, such as transcripts

5. Student Financial Services:
   a. Responding to requests for information concerning student accounts
   b. Issuing 1098-T documents
   c. Accepting credit card payments

6. Human Resources:
   a. Educating employees on the University's Identity Theft Program at employee orientation
   b. Changing addresses and other employee information
   c. Verifying identifying documents for new employees
   d. Conducting background checks on new employees
   e. Issuing Flexible Spending Account (FSA) cards

7. Payroll:
    a. Responding to requests for payroll information
    b. Disbursing payroll
    c. Issuing tax documents and reports

8. Technology Services:
    a. Assessing technology risks and weaknesses
    b. Maintaining all computer and data base access passwords

G. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University will make reasonable effort 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.