RESOLUTION TO ADOPT IDENTITY THEFT POLICY

WHEREAS, in late 2008 the Federal Trade Commission (FTC) and federal banking agencies issued a regulation known as the Red Flag Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 with the intention of reducing the risk of identity theft by requiring stronger fraud prevention to protect consumers' personal data,

WHEREAS, the Red Flag Rule has identified a "Red Flag" as a pattern, practice or specific activity that indicates the possible existence of identity theft and applies to any organization that offers credit or manages a "covered account," and

WHEREAS, The Red Flag rule requires any organization that maintains a "covered account" to establish, document, and maintain an identity theft prevention program that identifies potential Red Flags, detects the occurrence of Red Flags, and appropriately responds to Red Flags, and

WHEREAS, the Red Flag Rule has identified "covered accounts" which involve such activities including maintenance of student account information, acceptance of credit cards for payments, student tuition payment plans, and credit and employee background checks, and

WHEREAS, the Administration has developed an Identity Theft Prevention Policy attached as Exhibit A, and

WHEREAS, the administration recommends that said Program be adopted by the Board of Trustees,

NOW THEREFORE BE IT RESOLVED, Board of Trustees adopts the Identity Theft Prevention Policy as shown on Exhibit A.

Holly C. Stern

_____

Holly C. Stern, Esq.
General Counsel and
Secretary to the Board of Trustees
New Jersey Institute of Technology

April 9, 2009
Board Resolution 2009-17

Exhibit A

New Jersey Institute of Technology

Identify Theft Prevention Program Policy

Purpose

This policy is adopted pursuant to the Fair and Accurate Credit Transactions Act and federal regulations promulgated at 16 CFR § 681.2, which requires certain organizations, including NJIT, to provide an identity theft program. The regulations call a pattern, practice, or specific activity that indicates the possible existence of identity theft a "Red Flag"

By adoption of this policy, the University will make reasonable efforts to protect the personal identification and financial information it creates, receives, maintains and transmits, and to comply with current laws that provide for the protection of these types of information.

Background

The Federal Trade Commission (FTC) and federal banking agencies issued a regulation known as the Red Flag Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The regulation is intended to reduce the risk of identity theft by requiring stronger fraud prevention to protect consumers' personal data. The regulation applies to any organization that offers credit or manages a "covered account" (as defined below). The Red Flag rule requires any organization that maintains a "covered account" to establish, document, and maintain an identity theft prevention program that identifies potential Red Flags (as defined below), detects the occurrence of Red Flags, and appropriately responds to Red Flags.

A "Red Flag" is defined as a pattern, practice or specific activity that indicates the possible existence of identity theft. Examples of "Red Flag" incidents include presentation of suspicious identity documents or frequent address changes.

Application to New Jersey Institute of Technology's Accounts

A "covered account" is defined as (i) an account is designed to permit multiple payments or transactions; and (ii) any other account maintained by the university for which there is a reasonably foreseeable risk to the university, students, or employees from identity theft, including but not limited to financial, operational or compliance risks. NJIT is subject to the Red Flag rule because the university participates in or offers:

- Student tuition and fee payment plans
- The Federal Perkins Loan program
- Background checks on select employees
- Extensions of credit by use of credit cards for payments to NJIT for services.

Definitions

For purposes of this policy, the following definitions apply:

(a) For NJIT, the following activities are covered:
- Student tuition and fee payment plans and records maintained in support of these plans;
- Student Loan Programs, including The Federal Perkins Loan Program;
- Extension of credit by use of credit cards for payments to NJIT for services;
- Credit and background checks used in the hiring procedure, and
- Access to university, employee, and/or student records that may be defined as being "any other account", as defined in Application to New Jersey Institute of Technology's Accounts, above.

(b) 'Credit' means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

(c) 'Creditor' means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunications companies.

(d) 'Identity theft' means a fraud committed or attempted using identifying information of another person without authority.

(e) 'Notice of Address Discrepancy' means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. § 1681(c)(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

(f) 'Person' means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(g) 'Personal Identifying Information' means a person's credit card account information, debit card information bank account information and drivers' license information and for a natural person includes their social security number, mother's birth name, and date of birth.

(h) 'Red flag' means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(i) 'Service provider' means a person or vendor that provides a service directly to the university.

Prevention and Mitigation of Identity Theft.

In the event that any university employee directly responsible for the handling of covered accounts becomes aware of red flag activity indicating possible identity theft, such employee shall notify his or her supervisor. If the supervisor determines that further action is necessary, one or more of the following responses may be performed:

- Determination that no response is warranted under the particular circumstances.
- Notify of the Senior Vice President for Administration and Treasurer.
- Deny access to the covered account until other information is made available to eliminate the red flag.
- Contact the affected student or employee.
- Change any passwords, security codes or other security devices that permit access to the covered account in question.

Red Flag activity that may be indicators of possible identity theft shall include, but not be limited to:

(1) Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of such alerts are:
   a. A fraud or active duty alert that is included with a consumer report
   b. A notice of credit freeze in response to a request for a consumer report
   c. A notice of address discrepancy provided by a consumer reporting agency

(2) Suspicious documents. Examples of suspicious documents include:
   a. Documents provided for identification that appears to be altered or forged.
   b. Identification on which the photograph or physical description is inconsistent with the appearance of the individual offering such identification.
   c. Identification on which the information is inconsistent with information currently or previously provided by the individual offering such identification.
   d. Identification on which the information is inconsistent with readily accessible information that is on file, such as a signature card or a recent check; or
   e. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

(3) Suspicious personal identifying information. Examples include:
   a. Personal identifying information that is inconsistent with external information sources used by the university. For example:
      i. The address does not match any address in the consumer report; or
      ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
   b. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the university.

c. Other information provided, such as fictitious mailing address, mail drop addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.
d. The use of a SSN, address, or telephone number that is the same as that belonging to another person.
e. Where a person is required to submit an application or registration to the university and fails to provide all required personal identifying information and later does not provide all required personal identifying information in response to notification that the application or registration is incomplete.
f. Personal identifying information is not consistent with personal identifying information that is on file with the university.

(4) Unusual use of or suspicious activity relating to a covered account. Examples include:
a. Shortly following the notice of a change of address for an account, there is a request for the addition of authorized users on the account.
b. An account is used in a manner that is not consistent with established patterns of activity on the account, such as:
i. Nonpayment when there is no history of late or missed payments;
ii. A material change in purchasing or spending patterns.
c. An account that has been inactive for a long period of time is used.
d. University mail sent to a person is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's account.
e. The university is notified that a person is not receiving paper account statements.
f. The university is notified of unauthorized charges or transactions in connection with an account.
g. The university is notified by that an account has been opened by a person known or suspected to be engaged in identity theft.

(5) Notice from students, employees, law enforcement, or other reliable sources regarding possible identity theft or fraudulent activity relating to covered accounts.

Updating the Program

The University shall annually review and, as deemed necessary, update the Identity Theft Prevention Policy in order to reflect changes in risks to students, employees, and university covered accounts.

Program Administration

The Senior Vice President for Administration and Treasurer is responsible for administration of the Identity Theft Prevention Policy. The Director of Internal Audit will report to Board of Trustees annually on compliance with the red flag requirements.

University departments, under the auspices of the Senior Vice President for Administration and Treasurer, will administer training to employees on the Identity Theft

Prevention Policy, protection of confidential data, and prevention of fraudulent "Red Flag" activity.

Outside Service Providers

Service providers engaged to perform an activity in connection with one or more covered accounts shall provide documentation to the University that their activities are conducted in accordance with laws, regulations, and policies designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.