HARRISBURG UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Office of Institutional Compliance

IDENTITY THEFT PREVENTION PROGRAM

In accordance with the Federal Trade Commission "Red Flags Rule"

Approved by the Board of Trustees - May 14, 2009

Harrisburg University of Science and Technology

Identity Theft Prevention Program

The Harrisburg University Identity Theft Prevention Program ("the Program") includes routine monitoring activities as a "creditor" as defined by the Federal Trade Commission (FTC) because students are permitted to pay tuition obligations due to the University over an established period of time. While the level of identity theft risk associated with the relevant covered accounts is relatively low, implementation of the Program is required nonetheless for all students.

There are four (4) functional areas of the University responsible for monitoring information and activities that could expose the University to potential identity theft risk and liability:

- Financial Aid Office
- Student Accounts Office
- Office of Records and Registration
- Office of Information Systems

Financial Aid Office
This office collects and maintains documents and information where an incident of identity theft could occur.

The Free Application for Federal Student Aid (FAFSA) requires specific information including student and parent(s) name, address, Social Security Number, dates of birth, mother's maiden name (in certain instances), citizenship status or Resident Alien Identification Number and status, Selective Service registration status, and income information. The documents that result from the FAFSA application, a Student Aid Report (SAR) or electronic Institutional Student Information Record (ISIR), also contain all of the information reported on the FAFSA. One of these output documents must be maintained in the Financial Aid Office.

Additionally, student loan applications and Master Promissory Notes also contain specific personal information about the borrower and co-borrower that must be protected.

Protection of electronic data and information maintained by the Financial Aid Office is covered under the Office of Information Services section of this Program.

Procedures taken to prevent a loss in the Financial Aid Office include:
Locking file cabinets containing student files, reports and rosters;
Locked door with very limited key access; and the
Use of a document disposal contractor to discard unneeded documents.

The relevant "red flags" that could occur in the Financial Aid Office are, for example:
Name and address discrepancies for the student or parent(s);
Personal information inconsistent with information already on file; or,

Any unusual or suspicious request for information.

Student Accounts Office

This office collects and maintains documents and information where an incident of identity theft could occur.

Use of a credit card is one method of payment for tuition and other charges at the University. Credit card information can be obtained by telephone and recorded on a document or an authorization form with credit card information can be received via facsimile machine. In both instances, the University can be at risk not only for fraudulent use of an unauthorized party's credit card information, but also for the potential theft of credit card information documents.

Protection of electronic data and information maintained by the Student Accounts Office is covered under the Office of Information Services section of this Program.

The relevant "red flags" that could occur in the Student Accounts Office are, for example:

Name and address discrepancies for the student, parent or third party payment;
Personal information inconsistent with information already on file; or,
Any unusual or suspicious request for credit card payment or refund information.

Procedures taken to prevent a loss in the Student Accounts Office include:

Confirming the identity of the person making the payment with the credit card used;
Locking file cabinets containing payment documents, reports and rosters;
Locked door with very limited key access;
Use of a document disposal contractor to discard unneeded documents; and
Online payment options or the use of a credit card machine to reduce the paper documents containing credit card information.

Office of Records and Registration

This office collects and maintains documents and information where an incident of identity theft could occur.

The Application for Admission to the University requires specific information including student and parent(s) name, address, Social Security Number, date of birth, mother's maiden name (in certain instances), citizenship status or Resident Alien Identification Number and status, and other information.

Protection of electronic data and information maintained by the Office of Records and Registration is covered under the Office of Information Services section of this Program.

Procedures taken to prevent a loss in the Office of Records and Registration include:

Locking file cabinets containing student files, reports and rosters;
Locked door with very limited key access; and the
Use of a document disposal contractor to discard unneeded documents.

The relevant "red flags" that could occur in the Office of Records and Registration are, for example:

Name and address discrepancies for the student or parent(s);
Personal information inconsistent with information already on file; or,
Any unusual or suspicious request for information.

Office of Information Services

The Office of Information Services (OIS) is responsible for the maintenance and security of data and information communicated over the university's network or held electronically in the university's Enterprise Resource Planning (ERP) system. Accordingly, OIS takes considerable identity theft protection measures in order to identify and prevent unauthorized access to University systems.

The relevant "red flags" that could occur in the Office of Information Services are, for example:

- Attacks on the computing system using malicious viruses;
- Unauthorized use of another person's User ID and Password information; or,
- Any unusual or suspicious request for access to data outside an employee's assigned security access level.

Procedures taken to prevent identity management in the Information Services area are:

Policy Development and Enforcement

University policies have been developed in order to frame the OIS security program. Namely among these are The ERP Access and Security Policy, The Responsible Use of Computing Policy, and The Anti-Spam Policy.

Firewalls

Dedicated redundant firewall appliances separate University servers from the public Internet and the University's ERP. The firewalls use NAT (network address translation) to hide the servers' true addresses from the outside and to only allow specifically designated traffic to reach the servers. The firewalls are configured to reject unauthorized traffic. Any unusual activity is captured in daily generated logs. The firewall configuration is periodically reviewed to ensure that rules and policies are up-to-date.

Anti-Virus, Anti-Malware, and Anti-Spyware Software

University servers, and all client workstations which have access to those servers, are protected by anti-virus, anti-spyware, and anti-malware software. Virus definitions are updated on a regular basis. Logs are generated to ensure that the anti-virus, anti-spyware, and anti-malware software is functioning properly, that updates are occurring, and that no unusual activity is taking place. Email alerts are triggered in case of problems.

Encryption of Data In-Transit

Data transmitted between the University and outside points is encrypted to protect against eavesdroppers. Batch file transfers between the University and authorized outside parties

are protected by SSH, SSL, or IPSec VPN.

Encryption of Stored Data

Passwords are hashed for storage using the SHA algorithm.

Maintaining System Patches

The OIS network administrators are responsible for maintaining patch levels on all servers and firewalls. The administrators subscribe to appropriate vendor mailing lists which announce the availability of new patches. When a patch is released, the administrators test it on servers outside of the University environment to ensure that it will not interfere with proper system operations. The administrators also evaluate the severity of the risk being patched. Once the patch has been tested and evaluated, it is scheduled for implementation in the production environment.

Intrusion Detection System

An Intrusion Detection System (IDS) monitors the network, continuously looking for malformed packet attacks and logs suspicious activity.

Penetration Testing and Perimeter Scanning

The University contracts annually with an independent consultant to conduct penetration testing and perimeter scanning in order to evaluate the security of the network by simulating an attack by a malicious user and scanning the network for active IP addresses, open ports, or vulnerable applications.

Logging

Significant events occurring on servers and network devices are logged. Logs are archived so they can be accessed for future research if needed.

Login and Password Controls

Controls are in place to ensure that passwords meet minimum complexity requirements and are changed on a regular basis. Additional controls lock accounts after a pre-determined number of failed logins. Timeouts either log a user out or lock a terminal after a certain period of inactivity.

Physical Security and Access Control

Security measures are designed to ensure the physical security of the University servers. Access to the servers is limited to essential personnel only. Access to the servers is controlled by card key.

Document Control

Creating hard copy documents containing sensitive information is avoided when possible. When no longer needed, documents containing sensitive information are shredded.