HARRISBURG UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Office of Institutional Compliance

INFORMATION SECURITY
AND
SECURITY BREACH NOTIFICATION PLAN

In accordance with the Pennsylvania "Personal Information Notification Act"

Harrisburg University of Science and Technology

Information Security and Security Breach Notification Plan

POLICY

It is the policy of Harrisburg University of Science and Technology to comply with Pennsylvania Senate Bill 712, effective June 20, 2006, entitled the "Personal Information Notification Act."

PURPOSE OF THE PLAN

This plan sets forth the duties and responsibilities of institutional employees to:

Implement and maintain measures to prevent unauthorized access to personal information;
Identify when a security breach has occurred;
Establish the responsible parties to initiate the notification process

DETAILS OF THE NOTIFICATION ACT

The Act applies to entities doing business in Pennsylvania that maintain, store or manage computerized databases that include personal information of multiple individuals. Those entities must promptly notify Pennsylvania residents if their unencrypted and unredacted information was or is reasonably believed to have been compromised by a breach of security and such breach will cause injury to a Pennsylvania resident. If residents' personal information was stolen while encrypted, notice must still be provided if the security breach allowed an unauthorized person to access the data in an unencrypted form. A vendor that manages such data on behalf of a customer is only responsible for notifying that one customer.

Personal Information

The Act defines personal information as an individual's name linked with her or his Social Security number, driver's license or state identification card number, or information that would permit access to that individual's financial account. Personal information does not include information made publicly available from government records.

Required Notice

Entities may provide notice by mail, email, or over the telephone, with some caveats meant to ensure receipt of the notice. "Substitute notice" may be used if the entity needs to notify more than 175,000 people, the cost of notification would exceed

$100,000, or the entity lacks sufficient contact information. Substitute notice consists of posting notice on the entity's Web site, notifying major statewide media, and emailing notice upon acquisition of valid email addresses. Any entity notifying more than 1,000 people of a single breach must also promptly notify consumer reporting agencies of the timing, distribution and number of notices.

Exceptions

The Act carves out several exceptions. If a law enforcement agency advises an entity in writing that notification under this Act will impede an investigation, the entity must give notice only after the agency has determined that the notice will not compromise the investigation or security. Financial institutions meet the requirements of the Act by complying with the notification rules under the Federal Interagency Guidance on Response
Programs for Unauthorized Access to Customer Information and Customer Notice. Similarly, complying with notification rules promulgated by an entity's primary or functional federal regulator will meet the entity's duties under the Act. If an entity complies with its own preexisting notification procedures, and those procedures are consistent with the notification requirements of the Act, the entity has met its duty under the Act.

Remedies

Violations of the Act also violate the Unfair Trade Practices and Consumer Protection Law (UTPCPL). No private cause of action is allowed under the Act or the UTPCPL for a violation of the Act; only the Office of Attorney General can bring such an action.

PERSONAL INFORMATION PROTECTION MEASURES

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 protection measures in order to identify and prevent unauthorized access to University systems.

Procedures taken to protect personal information 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, SFTP 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 Prevention System
An Intrusion Prevention System (IPS) 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.

IDENTIFICATION OF A SECURITY BREACH

It is the responsibility of the **Director of Technology Services** to implement and maintain various detection tools to identify and document when, where and how a security breach occurred.

COORDINATING ADMINISTRATOR

Should a data security breach be confirmed, the **Director of Institutional Compliance and Reporting** is to be notified immediately to coordinate and document the execution of the Notification Plan. Any and all personnel needed to execute the Plan will temporarily serve under the direct supervision of the **Director of Institutional Compliance and Reporting** until the security breach event and notification to the affected parties is concluded.

NOTIFICATION PROCEDURE

A determination will be made on a case-by-case basis as to the appropriate response needed and the method of contact to be used for notification (mail, email, or telephone), as required by the statute. Each individual notification must be documented and preserved.

The notice shall contain:

- An indication that the communication is URGENT;
- Name and contact information at the University;
- Description of the categories of personal information that were or believed to have

been, acquired by a person without valid authorization; and,

- Specific elements of personal information and private information were, or believed to have been, so acquired.

RECORD RETENTION

All records relating to an incident shall be maintained for a minimum of seven (7) years in the event an adverse action occurs subsequent to the incident that may impact the affected party's credit standing with any cognizant credit reporting company.

SUMMARY REPORT OF THE EVENT

A summary report of each security breach incident shall be prepared by the **Director of Institutional Compliance and Reporting** within ten (10) business days following the conclusion of the event and notification has been completed. This report shall be distributed to the President, Provost, and AVP for Information Services.

EVALUATION OF PROCEDURE EFFECTIVENESS

The Information Security and Security Breach Notification Plan shall be evaluated on a biennial basis.

Approved: May 2009