Office of Information Services

Securing Harrisburg University's Digital Assets[1]

September 2008

Purpose: This document outlines steps taken by the Office of Information Services to protect and secure HU's digital assets (administrative, financial, academic, personnel, or student information).

- **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 Acceptable Use of Information Technology Policy, and The Anti-Spam Policy. All employees sign a confidentiality policy upon employment (see Employee Handbook). All HU employees (including students) are responsible for complying with confidentiality requirements such as FERPA, HIPAA, GLBA, and the Donor's Bill of Rights.

- **Firewalls:** Dedicated redundant firewall appliances separate University servers from the public Internet and the University's ERP (Jenzabar is the university's "one source of truth" administrative database in which the library imports its patron information). 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

[1] This document was created in response to the Federal Trade Commission's "Red Flag Rule" intended to reduce the risk of identity theft. It is an excerpt of a HU document entitled "Identity Theft Prevention Program". Questions about campus-wide identity theft issues should be address to HU's Director of Institutional Compliance and Reporting.

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.