University of Pittsburgh

To: Deans, Directors, and Department Chairs

From: Jerome Cochran, Executive Vice Chancellor

James V. Maher, Provost and Senior Vice Chancellor

Date: May 3, 2007

Subject: Security Controls

Electronically stored academic, administrative, and research information is a critical University resource. Threats from computer hackers and malicious software and attempts to steal sensitive information jeopardize the confidentiality and integrity of this resource. The consequences to the University from a compromise of our electronic data could be widespread and damaging.

Computing Services and Systems Development has established security controls such as network firewalls, antivirus software, and highly secure enterprise email and web site services. These services are centrally funded and managed, and, when implemented comprehensively, will significantly reduce security vulnerabilities.

Unfortunately, not all University departments have adopted these services. As a result, over the past year the number of compromised departmental systems has increased dramatically. Compromises to departmental systems are dangerous to the department itself and for the entire University since such compromised systems can provide access to other networked resources.

Given the acceleration in the number and types of security risks facing computer systems at the University, all departments will now be required to move to enterprise email, web services and network firewalls operated by CSSD.

The following is a brief description of these services:

- **Network Firewalls.** A network firewall provides the highest level of protection from Internet-based attacks. Network firewalls control network access to services on protected University computers. They also help monitor network activity that may be of a malicious nature. Network firewalls are required by several Federal regulations, including HIPAA, GLB, and Sarbanes Oxley.

- **Enterprise Email.** Enterprise email systems, either IMAP or Exchange, offer powerful, redundant hardware and software that permits a high level of reliability, standard email backup and retention policies, enterprise spam and virus protection software, and strictly monitored security controls.

- **Enterprise Web Service.** Enterprise web hardware and software offer closely monitored security controls and offer high level availability through redundant hardware and software.

Moving all University units to these enterprise services will take several months. Computing Services and Systems Development will be coordinating the process with each department to ensure a smooth transition. Once a comprehensive schedule has been developed, you will be contacted by CSSD regarding the implementation of these security services in your unit.

In addition, CSSD is able to provide a hosting service for unit-operated servers at its highly secure and closely monitored RIDC computer facility. Unlike the services listed above, which because of their criticality are centrally funded, a very reasonable cost model has been implemented to recover the cost of providing the service at RIDC. This is a very cost effective and highly secure solution for securing departmental servers that contain sensitive data. We recommend that you consider relocating servers to RIDC if the data they contain would benefit from a more secure location, one which would also relieve you of the need to maintain the hardware and software.

For additional information about the implementation of this security requirement, please contact CSSD by sending an email to Jinx Walton at jpw@pitt.edu.