University of Pittsburgh

Office of Finance

2409 Cathedral of Learning
Pittsburgh, PA 15260
412-624-6620
Fax: 412-624-4384

To: Deans, Directors and Department Chairs

From: Robert F. Pack RFP
Arthur G. Ramicone AGR

Date: October 11, 2010

Subject: Payment Card Industry Data Security Standards (PCI DSS)

As an organization that accepts payment cards (e.g., debit and credit cards), the University of Pittsburgh is obligated to protect the data involved in those transactions. In order to ensure that this sensitive data is protected, the University is now undertaking an assessment of its Information Technology assets and the business methods related to payment card processing. To accomplish this project as efficiently as possible, a third-party qualified security assessor, ParenteBeard, LLC, has been engaged to assist in this review and remediation process, as well as to assist us in establishing appropriate policies and procedures for our ongoing reviews. Any department that collects, transmits, stores or processes payment card information (e.g., debit and credit cards) will be within the scope of this review.

This project will be completed in two phases. The first phase will be the assessment of the various University systems and payment card processes in place at the school or department level in order to analyze them for compliance with the PCI DSS and identify any vulnerability. The cost of this phase will be handled centrally.

Upon completion of the assessment of each area within the University, we will then immediately begin the process of remediating any deficiencies which may exist in that area. The cost of the second phase, however, will be absorbed by each department based on their specific remediation needs. Unfortunately, it is impossible to determine the cost associated with the remediation needed within an individual area until the assessment phase is completed for that particular area.

Implementation of the PCI DSS project is imperative. It is far less expensive and places the University in a much stronger position by being certified PCI compliant before an adverse event occurs. Penalties are severe not only from the payment card industry, but also from legislation such as the Pennsylvania Data Breach Act as well as damage to the University's reputation through significant negative publicity. A security breach could result in the University losing its ability to accept credit cards on campus and PCI certification would be required to continue card acceptance. Increased costs resulting from annual third party audit reviews, card re-issuance fees, forensic investigations, notification of victims and remediation costs, and the potential for fines of as much as $500,000 are also likely.

The project team consists of representatives from the following University offices: Office of Finance, Computing Services & Systems Development, Financial Information Systems, Internal Audit and the Office of General Counsel. The University's project managers will contact appropriate persons within your individual organization within the next several weeks to provide details of this project and to request more specific information about PCI-related activity within that school or department. We ask that you and your staff provide them with your full cooperation to ensure that the assessment and remediation is completed in a timely fashion.