THE
UNIVERSITY
OF UTAH

Jeffrey J. West
Associate Vice President

Financial and Business Services
201 South Presidents Circle, Rm 408 Salt Lake City, Utah 84112 (801) 581-7520 FAX (801) 585-5257

TO: Deans, Directors, and Department Chairs

FROM: Stephen H. Hess, Chief Information Officer SHess

Jeffrey J. West, Associate Vice President JWest

DATE: July 18, 2008

RE: Credit Card Compliancy Requirements

The increased acceptance and usage of credit card payments on campus has been accompanied over the past few years by significant initiatives within the credit card industry to address the safety and security of processing and maintaining card information. As a result, any entity accepting credit cards must comply with these on-going security requirements in order to continue to accept credit cards. These stringent security requirements are necessary to assist in preventing fraud and misuse of personal data.

The Payment Card Industry (PCI) Security Standards Council is an organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The PCI Data Security Standard (PCI DSS) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. Compliance with these standards is mandatory for any entity accepting credit cards as payment for goods or services. Consequences for non-compliance include significant fines and penalties, legal risk, negative impact on the University's public image should a security breach occur where personal credit card data is compromised, and potential loss of the University's ability to accept credit cards. Therefore, the University, and all its departments, must comply with all requirements spelled out in these standards.

In an effort to do this, all departments accepting card payments through use of credit card machines, point of sale equipment, e-commerce through the internet, third-party payment processors, or via any other means will be receiving a packet of information on how to get into compliance and maintain that status. These packets include an agreement to be signed and a questionnaire to be completed annually. Departments must also provide copies of their written reconciliation process that should be updated as needed, and should also keep contact personnel and information updated as needed. All of this information and documentation will be collected, maintained, and monitored by the Income Accounting and Student Loan Office (http://fbs.admin.utah.edu/index.php/income/ or 585-5686). All questions or issues related to the acceptance and processing of credit cards, including requests for new accounts, should be directed to that office.

Departments using equipment with internet connections, point of sale equipment, third-party processing software on a server or computer, or the use of software that allows any type of credit card information to pass through a server or computer, may need to have this equipment scanned monthly. This is determined by the Compliance Office of OIT. Your support and cooperation is essential to the University's compliance with these standards and conformance with best business practices for handling credit card transactions.