

PCI-DSS

Standard for Processing Transaction
with Cardholder Data

24 March 2008



Introductions

- Andrew Mangels, Controller
- Tom Mathers, Associate Controller/Bursar
- Jacqui Watrous, Administrative Systems Director
- Christopher Misra, Network Analyst

PCI-DSS

- Payment Card Industry - Data Security Standard
 - Currently Version 1.1
- A security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
 - Founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International.
- Self-Assessment questionnaires have been updated to comply with the 1.1 Standard

PCI-DSS: What it means

- The University is now required to comply with Payment Card Industry (PCI) Standards due to the number of transactions that are processed
 - We must be in full compliance by 1 June 2008
- Campus members must complete an annual self assessment questionnaire (survey)
 - These have changed since we last met
- Quarterly scan of IP addresses that store, transmit, or process cardholder data
 - Only relevant for a limited number of cases on campus

PCI-DSS: Why you are here

- Your department has been identified by the Treasurers office as one that accepts credit cards
 - You have completed the first survey(s) designed to document how you process and store credit card data
 - There have been updates to University policies and procedures
 - The questionnaires have changed, each department which accepts credit cards must complete new questionnaires that pertain to your operations, and we hope to clarify what that means

PCI-DSS: Why we are here

- To review the progress made since we last met
 - Updates to POS Terminals
 - Policy and Procedure changes and updates
 - Changes to Business Records Retention requirements
 - Review of the new questionnaires
- To ensure that the campus is in compliance with the regulations
 - We are required to be in full compliance by June
- To answer any questions that you may have

PCI-DSS: Updating POS terminals

- This update includes the account number truncation software and also updates for the MasterCard, Visa and American Express interchange
- Limits receipts to only printing the last four digits of the credit card
- These updates are available and have been implemented by many on campus so far

PCI-DSS: University Policy

- The University eCommerce committee has drafted a set of principles to guide compliance.
 - These are the University's interpretation and extension of PCI-DSS
- These have been formed as a new University Policy on the Acceptance of Credit and Debit cards
 - This policy will be promulgated shortly
 - This has also resulted in University Fiscal Procedures
- The Controller's office has also published a draft credit card policy for campus
 - We will review this document here

PCI-DSS: Reviewing the Questionnaires

- Our initial approach was to create (3) distinct questionnaires based from the version 1.0 SAQ for PCI security standards council
 - However, the relevant security standard was version 1.1
- Currently, the self-assessment questionnaires have been updated to comply with version 1.1 of the PCI-DSS
- There are now (4) questionnaires:
 - A,B,C,D
 - Most here will use questionnaire B, but we need to verify

PCI-DSS: Reviewing the surveys

- If you are processing cardholder data with only a POS (Point-of-Sale) terminal, then likely you will have to fill out questionnaire B
 - *Imprint Machines or Stand-alone Dial-out Terminals Only, no Electronic Cardholder Data Storage*
- Then there are (4) requirements that have to be fulfilled under PCI-DSS:
 - Requirement 3: Protecting Stored Data
 - Requirement 7: Restrict access to data by business need-to-know
 - Requirement 9: Restrict physical access to cardholder data
 - Requirement 12: Maintain a policy that addresses information security for employees and contractors.

PCI-DSS Timelines

- The University is subject to several compliance deadlines.
 - *December 15 2007*
 - *Completed Prohibited Data Retention Attestation*
 - *Initial vulnerability scan results*
 - *Completed Self-Assessment Questionnaire (SAQ)*
 - *31 March 2008*
 - *Initial SAQ to bank*
 - **1 June 2008**
 - **Completed, passing SAQ and vulnerability scan results to President's Office**

PCI-DSS: Relevant Links

- PCI-DSS

<https://www.pcisecuritystandards.org/>

- Self-Assessment Questionnaires

- These can be hard to find

<https://www.pcisecuritystandards.org/tech/instructions.htm>

- Campus data compliance web pages

<http://www.oit.umass.edu/security/compliance/index.html>