

PCI-DSS

Standard for Processing Transactions
Credit Card Data

5 March 2009



Introductions

- Andrew Mangels, Controller
- Tom Mathers, Associate Controller/Bursar
- Jacqui Watrous, Administrative Systems Director
- Christopher Misra, Information Security Officer

PCI-DSS

- Payment Card Industry - Data Security Standard
 - Previous version 1.1 was used for the 2008 PCI-DSS compliance process.
 - Current version is 1.2
- A security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.
- Self-Assessment questionnaires have been updated to comply with the 1.2 Standard

PCI-DSS version 1.2 changes

- https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_v1-2.pdf
- Mostly clarifications of v1.1 standard
- Major Changes
 - Requirement 6.6 is now mandatory
 - Impacts SAQ D
 - “requiring all public facing Web applications to be reviewed either manually or with automated assessment tools or protecting them by installing a Web application firewall”
 - WEP is no longer acceptable for wireless
 - Patching must be applied on a risk basis

PCI-DSS: What it means

- The University is required to comply with Payment Card Industry (PCI) Standards
 - We must perform annual compliance checks
 - We operate on a June annualized schedule
- Campus users who process credit cards must complete an annual Self Assessment Questionnaire (SAQ)
 - These have changed since we last met
- Quarterly scan of IP addresses that store, transmit, or process cardholder data

PCI-DSS: Why you are here

- There is now a new version of the PCI-DSS standards
- Your department has been identified by the Treasurers office as one that accepts credit cards
 - You have completed the previous annual survey(s) designed to document how you process and store credit card data
 - 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 ensure that the campus is in compliance with the regulations
 - We are required to be in full compliance by June
- To clarify the changes with the PCI-DSS version 1.2
- To answer any questions that you may have

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 principles are outlined in the University Policy on the Acceptance of Credit and Debit cards
 - This policy has previously been promulgated
 - There are also University Fiscal Procedures
- The Controller's office has also promulgated credit card policy for campus
 - We will review this document here

PCI-DSS: Reviewing the Questionnaires

- The self-assessment questionnaires have been updated to comply with version 1.2 of the PCI-DSS
- There are now (4) relevant questionnaires:
 - Most here will use questionnaire B, but we may need to verify
- If you have deployed a new method of taking credit cards, you may be subject to a different SAQ

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

University compliance deadlines.

- **1 June 2008**
 - **Completed, passing v1.1 SAQ and vulnerability scan results to President's Office**
- **30 April 2009**
 - **Completed passing SAQ returned to A&F systems**

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>