F & A Monthly Meeting

Campus Banking 3.10.26

UMass Boston

eCommerce – PCI Compliance & Annual Campus Audit

- PCI
  - PCI Definition
  - Compliance requirements
  - Consequence of non-compliance
- Umass – Annual PCI audit
  - Timeline
  - Roles
  - Process

UMass Boston

PCI (Payment Card Industry)

- What is it?
  - Set of standards and requirements by the PCI council that ensures all companies that process, store or, transmit card information, maintain a secure environment.
  - Goal
    - Protect card holder data
    - Prevent fraud and data breaches
    - Reduce payment risk
    - Ensure secure payment flow

UMass Boston

PCI (cont'd) – PCI DSS requirements

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

UMass Boston

PCI (cont'd) - Do/don't examples

- Protect cardholder data (req 3&4)
  - DO NOT email credit card numbers
  - DO NOT store card data on local computers
  - DO NOT keep unsecured paper forms with cc numbers
- Develop and maintain secure system (req 6 & 11)
  - DO perform vulnerability scans (IT security)
- Identify and authenticate access (req 8)
  - DO use SSO (single sign-on) or MFA (multi-factor authentication)

UMass Boston

PCI (cont'd) – Consequence of non-compliance

- Damage to public image
- Loss of sales and revenue
- Loss of customer confidence of online payment use
  - Increase in cash & check payment processing
- Fines and penalties

UMass Boston

Umass PCI Audit

- Audit Period
  - Feb – May
- Roles
  - QSA (Qualified Security Assessor)
    - Certified experts on all PCI matters
    - Review and assist w/ SAQ for selected stores
    - Ensures security controls are in place
  - Treasury (Central)
    - Coordinates system wide annual audit
    - Reviews final SAQ submission to Processor
    - Oversees merchant accounts
  - IT (Security team)
    - Performs quarterly vulnerability scans
    - Fills out IT section of SAQ
    - Ensures network and system security
  - Campus Banking (eCom reps)
    - Assists and ensures audit done timely
    - Coordiantes PCI & merchant related activity on campus
  - Campus Stakeholders
    - Fill out SAQ, complete PCI training, Provide AOC, Review POS serial & terminal #'s

UMass Boston

Umass PCI Audit

- Process Timeline
  - Audit preparation (Feb)
  - Audit/Assessment (March – April)
  - Completion & Submission (May)

UMass Boston

Questions?

Contact us at Campus.Banking@umb.edu

UMass Boston