PCI DSS- Compliance Reporting

Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

PCI (Payment Card Industry Data Security Standard)

- How is the Bursar's Office involved?

Karen A. Jones
Bursar/Assistant Treasurer
karen.jones@cincinnatistate.edu

College Stats

- 2 year Public
  - Over 130 degree and certificate programs (with 4 Bachelor programs)
- 9,710 student headcount as of 9/27/24 (up 11.2% YOY)
- 4 locations
- 5 Colleges/Divisions
  - Business Technology
  - Engineering & Information Tech
  - Health & Public Safety
  - Humanities & Science
  - Workforce Development
- 3 Full-Time Bursar/Cashier Office Staff
- Ellucian Colleague – recent SQL migration
- Touchnet – Third Party Payment Processor
- Bursar's Office became cashless during COVID

Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

PCI DSS
Compliance Reporting…

- What is it and why is the Bursar involved?
  - Stats on fraud
  - Assistant Treasurer responsibilities
- Benefits – helps mitigate fraud and reduce data breaches
- Requirements –
  - Firewall/Password Protection/Encryption/Restrict access
- FAQs

Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

PCI DSS – Defined

- The introduction of and scramble for a spot in the online shopping realm resulted in an increase in credit card fraud. In December 2004, the Payment Card Industry developed a set of security standards and controls designed to protect credit card information during and after a financial transaction. Before then, in 2001, Visa was the first major card network to develop its own set of security standards for companies that accept digital payments.
- The payment cards in scope of PCI DSS include debit, credit, and pre-paid cards branded from one of the 5 major card issuers: AmeX, Discover, JCB, MC, and Visa.
- PCI DSS covers a mandatory baseline of 12 requirements. Only when all 12 requirements are met is an organization considered PCI Compliant.
- Any organization that stores, processes, and transmits credit card information is required to be PCI compliant.

PCI DSS – Why is the Bursar involved?

- Of the 12 requirements covering 6 control objectives, the Bursar at Cincinnati State is responsible for:
- 4.2 Cardholder Data Protection
  - The College shall not permit the transmission nor communication of unencrypted credit card PAN (personal account numbers) data via end-user messaging technologies communication (text, e-mail, instant messaging, SMS, chat, and any social media application)
- 9.9 Devices – Inventory Maintenance and Policy Communication
  - The College will maintain an inventory of devices, routinely inspect each device, and train staff to recognize device tampering.
- 12.8 Third Party Payment Processors – Maintenance of Compliance Certificates
  - The College will maintain a list of all third party credit card processors' PCI DSS Compliance Certifications.

PCI CSS Compliance – Stats on Fraud

- **Key Credit Card Fraud Statistics (a dime for every $100 spent)**
  - **Total value of credit card fraud**: $246 million (2023)
  - **Annual global fraud losses (credit & debit card)**: $34.36 billion (2022)
  - **Total volume of credit card and debit card fraud losses**: 6.81 cents per $100 (2020) & 6.78 cents per $100 (2019)
  - **U.S. share of global payment card fraud**: 38.83% (payment card fraud losses) and 22.40% (transaction value)
  - **Projection for total losses due to payment card fraud from 2021-2023**: $408.50 billion
  - California wins with $38M in credit card fraud losses last year. OH is at $2.9M

PCI DSS – Benefits of Compliance

- Helps minimize fraud
- Is required by an organization's insurance provider. Cybersecurity policies require that an insured is PCI DSS Compliant
- Provides a level of assurance that an organization is a good steward of its client's information
- Eliminates penalties and fines levied by card issuing banks and payment processors. Fines as much as $50 to $90 per cardholder can be assessed in the event of a breach.

PCI DSS Compliance – How to get started

- https://www.auditboard.com/blog/pci-dss-requirements/

- This site is an excellent source of information providing the who, what, where, when, and why of PCI DSS Compliance.
- Steps followed by Cincinnati State:
- Committee formation
- Garner upper management support
- Step through each of the 12 requirements
  - Establish and communicate policies then “I have had read and understand requirements”

Best Practices

Examples of how the Bursar's Office can help maintain PCI Compliance:

- Stop taking CC payments in person or over the phone, if possible. Many TPVs offer "store fronts" eliminating the need to manually process CC payments
- If you don't need it, don't store it – Once a transaction has been processed, destroy the forms on which the cardholder data exists.
- Proper destruction – use a "cross-cut" shredder or contract with a Third Party document destruction vendor.
- Maintain a clean desk policy
- Secure your computer

Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

Training

https://www.pcisecuritystandards.org/program_training_and_qualification/requirements_awareness/

https://training.knowbe4.com/auth/saml/3d808b760c239

Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

Thank You!