What is PCI DSS?
The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements for credit card account data security, developed by the credit card industry in response to an increase in identity theft and credit card fraud. As a merchant who handles credit card data, Binghamton University is obliged to safeguard that information and adhere to the standards established by the Payment Card Industry Security Standards Council including setting up controls for handling credit card data, computer and internet security and completing an annual self-assessment questionnaire (SAQ).

Without adherence to the PCI DSS, the university would be in a position of great reputational risk and financial liability. Merchant account holders who fail to comply are subject to:

a) Fines imposed by the payment card industry.
b) Additional monetary costs associated with remediation, assessment, forensic analysis, or legal fees.
c) Suspension of the merchant account.

Prior to PCI DSS, each major credit card brand (Visa, MasterCard, Discover, American Express and JCB) had its own security requirements. Due to mounting losses from fraud and theft, PCI DSS was announced in September 2004, as a merging of each of the individual card standards. The DSS offered a single approach to safeguarding sensitive data for all card brands. This was actually quite an historic event, as these card brands are extremely competitive. For them to gather collectively demonstrates the magnitude of the problems they faced.

Did you know?
It is important to realize that compliance does not equal security. It’s analogous to locking the doors of your home, which is a core security component but does not guarantee that a break in will not occur. While compliant merchants have good controls in place to protect cardholder data, all employees must remain vigilant and ensure that card holder data remains protected at all times.

MARK YOUR CALENDAR!
PCI DSS Workshop
open to all merchants
November 24, 2014
9:30-11:00 am
FA 258
How can you help?

- Complete the PCI DSS Compliance on-line training module annually.
- Complete the appropriate Self-Assessment Questionnaire (SAQ) for your department annually.
- Shred documents containing card holder data after transaction processing.
- Lock up credit card terminals when not in use.
- Ensure you have signed confidentiality statement on file with HR
- Do NOT share user IDs and passwords among staff members.
- Use strong passwords when logging into payment applications and two factor authentication when possible.

PCI DSS is NOT Checkbox Security!

It is important to remember that compliance is an ongoing issue. Properly filling out the SAQ and answering each question appropriately only validates your department’s compliance on that day and time. To remain compliant, the objectives and requirements of the PCI DSS must be followed every day. The best advice for accomplishing this is to incorporate those requirements into your business-as-usual practices.

What if something goes wrong?

In the event that you expect a PCI data compromise and/or a breach, please contact the Information Security Officer (ISO) or another member of the incident response team immediately.

Incident Response Team:

Eric Backlund
ISO & Director of Risk Management/Admin Compliance
backlund@binghamton.edu
777-7475

Mike Hizny
ITS Assistant Director of Networking
mhizny@binghamton.edu
777-4739

Erin Neske
Director of Finance
eneske@binghamton.edu
777-4140

What Data Must be Protected?

- **Cardholder Data (CHD)**
  The primary account number (PAN) is the defining factor in the applicability of PCI DSS requirements. If PAN is not stored, transmitted, or processed then PCI DSS does not apply. If PAN is stored with other data obtained as part of the payment transaction such as, cardholder name, expiration date, and/or service code, then protection is required for all elements.

- **Sensitive Authentication Data**
  This is the magnetic stripe data, card validation code (CVC, CVV, etc.) and PIN Data. This data can NEVER BE STORED!