Welcome to the Financial and Operational Audit newsletter from the Financial and Operational Audit office. Please feel free to forward comments, questions or suggestions:

Larry Meyer, director  572-6117, meyerl3@nku.edu
Rachel Brueggen, staff auditor  572-1345, brueggenr1@nku.edu
Kristi Horine, staff auditor  572-1341, horinek1@nku.edu

What is Payment Card Industry Data Security Standards (PCI DSS) Compliance?

What Is It?
The PCI Standard is not a law! It’s a regulation created by payment card companies (MasterCard and Visa Card being the leaders) and enforceable under contractual obligations with these credit card companies. Members and merchants agree to abide by these standards under the terms of their contracts with payment card companies. The Payment Card Industry (PCI) Standard outlines the security requirements for transmitting, storing, accessing, or processing cardholder data.

What If We’re Not in Compliance?
If a member fails to immediately notify VISA or MasterCard Fraud Control of the suspected or confirmed loss or theft of any cardholder transaction information, the member will be subject to a penalty of $100,000 per incident. Members are subject to fines, up to $500,000 per incident, for any merchant or service provider that is compromised while not compliant at the time of the incident.

Needless to say PCI compliance is a big deal.

What Information CANNOT be Retained or Stored by Users
• PIN Number
• Data on Magnetic Strip
• Full Primary Account Number
• Card Verification Value (CVV)

6 Objectives of PCI Compliance
1. Build and maintain a secure network
   • Install and maintain a firewall configuration to protect data
   • Change vendor-supplied defaults for system passwords and other security parameters
2. Protect cardholder data
   • Protect stored data
   • Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks
3. Maintain a vulnerability management program
   • Use and regularly update antivirus software
   • Develop and maintain secure systems and applications
4. Implement strong access control measures
   • Restrict access to data to a need-to-know basis
   • Assign a unique ID to each person with computer access
   • Restrict physical access to cardholder data
5. Regularly monitor and test networks
   • Track and monitor all access to network resources and cardholder data
   • Regularly test security systems and processes
6. Maintain an information security policy
   • Maintain a policy that addresses information
What Should Departments Do?
A University committee has been formed to help us take the necessary steps to ensure we are in compliance with these standards. One step in this process is to identify departments who are accepting credit card payments. Committee representatives will be contacting each office that accepts credit card payments to discuss their procedures.

If your department or operation is considering the purchase of a system that will accept, process, transmit or store credit card information, such as credit card payment on web site or similar process, you need to contact the Office of Bursar Operations for more information. They can be reached at: 572-5204 or bursar@nku.edu

What is Records Management?
It is the systematic control of recorded information, regardless of format, from original creation to ultimate disposition.

Or more simply . . .
Knowing what you have, where it is, how long you need to keep it and applying that knowledge.

Records Can Include. . .
- Papers
- Books
- CDs
- Photographs
- Digital Files, including Email
- Audio or Video Recordings
- DVDs
- Maps

Records can be created and kept in a wide variety of formats. All NKU employees create and maintain records. But only a small portion of these records needs to be kept permanently. All employees should evaluate their records for retention at least annually.

Keep or Delete
How long you retain a record or group of records is based solely on its content not its format. The state maintains approved retention schedules that list records by their content or record series.