Accepting Credit Card Payments:

Payment Card Industry Data Security Standards Compliance

- Please turn off, or to vibrate, all cell-phones/electronics
- Expected course length: 1 Hour
- Questions are welcomed.

Who Created It?

&

What Is It?

Video Presentation

http://youtu.be/1boEXDVkKjU

http://www.youtube.com/watch?v=1boEXDVkKjU&feature=youtu.be

“The Council” (PCI SSC)

Payment Card Industry Security Standards Council (PCI SSC) an Open Global Forum launched 2006.

The council develops, maintains and manages the PCI Security Standards, which include the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) Requirements.

The Council’s five founding global payment brands (*American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.*) have incorporated the PCI DSS as the technical requirements for their data security compliance programs.

The Standards

PCI Security Standards are technical and operational requirements set by the PCI DSS

Anyone that accepts, process, transmits or stores any cardholder data

- Cashiers – Assistants
- Managers – Supervisor
- IT – Treasury

3 steps for adhering to the PCI DSS

(Common-sense steps that mirror security best practices)

- **Assess** is to take an inventory of your IT assets and business processes for payment card processing and analyze them for vulnerabilities that could expose cardholder data.
- **Remediate** is the process of fixing those vulnerabilities.
  (i.e. Testing & Annual Training)
- **Report** entails compiling records required by PCI DSS to validate remediation and submitting compliance reports to the acquiring bank and global payment brands you do business with.

  - This is a continuous process
    - 12 requirements

How do we Validate PCI DSS Compliance?

- Annual Self-Assessment Questionnaire (SAQ)
  - https://www.pcisecuritystandards.org/documents/pci_saq_c_v2.doc
- Annual Testing and Training
- Quarterly Network Scanning
  - Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV)
  - https://www.pcisecuritystandards.org/approved_companies_providers/index.php

The University of North Florida's Information Technology Services Office is tasked with fulfilling many of the PCI DSS Requirements and an essential key to the process.

However, it is the responsibility of all employees who may store, process, or transmit cardholder data to be aware of all of the PCI DSS requirements and use best practices when performing their assigned daily tasks.

Requirements and Security Assessment Procedures

Version 2.0 - October 2010

A full Introduction and PCI Data Security Standard Overview

- **https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf**

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data. It consists of common sense steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	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. Use 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. Assign a unique ID to each person with computer access 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

6 Goals & 12 Requirements

Goal #1

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Goal #2

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

File 13

NEW YORK POST

Confetti at Macy's Thanksgiving Day Parade contained police secrets

By SABRINA FORD, KAYLEE OSOWSKI and DAN MACLEOD
Last Updated: 6:20 AM, November 25, 2012
Posted: 1:18 AM, November 25, 2012

Charlie Brown wasn't the biggest loser at this year's Thanksgiving Day Parade.

Shredded police documents containing Social Security numbers, names of detectives and even a mention of Mitt Romney's Long Island motorcade rained down on revelers as part of the confetti used for the Macy's extravaganza.

Some of the material from the Nassau County Police Department remained scattered yesterday near Central Park West and West 65th Street — even as the department vowed a thorough investigation.

Paradegoer Ethan Finkelstein, of Manhattan, was amazed to find the information flying around.

"A friend of a friend was standing in front of me, and she had a big piece of confetti on her coat. She saw it had something on it, and we read it said SSN, like Social Security number," said the 18-year-old Tufts University freshman.

"We started picking all the confetti up, and it had all kinds of stuff — birth dates, addresses, account information.

"I don't know where it came from. All of a sudden it was everywhere!" said Finkelstein, who takes in the parade annually with his family.

"At first I thought it might be documents from Macy's employees until I saw that there were detectives' names and information about crimes in there. This is really shocking!"

It wasn't immediately clear how the files wound up as confetti.

Full Article
http://www.nypost.com/p/news/local/confetti_dential_B4seFCo8UzccaEN5KSx43N

*A few Security Tips

- Some Institutions Webpages or E-mail taglines make a formal request to customer(s). Such as:
  - “When emailing, please do not include personal information such as your account number, social security number, or other personal data.”
- Some Institutions develop a data retention and disposal procedure. Such as:
  - Do Not Store or Transmit cardholder data, or
  - Automated weekly purge of any such data

*A few Security Tips (continued)

- Some Institutions require before employees take breaks or leave for the day to take precautions: Such as:
  - When working with hardcopy information place in a secure file prior to leaving unattended
  - When working with electronic information “Lock” computer station prior to leaving unattended

At the Point of Sale … Are you Safe?

When a customer presents a credit card run the bases:

1. Check the card's security features to ensure that the card has not been altered.
2. Swipe the stripe to obtain authorization. Then check the authorization response and then take appropriate action.
3. Get the cardholder signature on the transaction receipt and compare the Name, Account Number, and Signature on the card to those on the receipt. They should match.

Are you Safe?

Why run the risk of accepting a counterfeit card? When you can simply *run* a check.
If you suspect fraud, make a Code 10 call:

1. Call the respective card's authorization center
2. Say, "I have a Code 10 Authorization request."
3. Follow the operator's instructions if you can do so safely.

"... and you're SAFE!"

Goal #3

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications

Goal #4

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Goal #5

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Goal #6

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security for all personnel

University Procedure and Best Practices*

- **PCI Compliance page**
  - http://www.unf.edu/anf/controller/PCI_Compliance.aspx
  - Credit Card Procedures and Best Practices
    - To download a copy click on the ***here*** link on this page

*Review these pages upon return to your office

University Procedure and Best Practices*

Are you holding a conference, selling merchandise or services? The University has a product that you can use!!

TouchNet® Marketplace™ is a comprehensive framework for enterprise-wide e.Commerce. It is used by campus departments and organizations to create, manage, and operate online storefronts and compliant payment systems for campus-developed web applications and other third-party business software. Marketplace helps centralize control of e.Commerce finances and technology while it distributes the management and operations of e.Commerce sites to authorized campus merchants.

- For questions, please contact Melissa Hyman in the Project Management Office at Ext 1122 or m.hyman@unf.edu

TouchNet® is a contributing member of the PCI Security Standards Council (PCI SSC) and is committed to Setting the Curve in safeguarding sensitive cardholder data. TouchNet is certified as both PCI DSS and PA-DSS compliant.

*Review these pages upon return to your office

University Procedure and Best Practices*

Check Vendor website

Allows you to verify is a 3rd party vendor is PCI compliant.

List of Validated Payment Applications

https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

*Review these pages upon return to your office

Penalties

A security breach can affect the UNF organization in profound ways:

- Fines
- Loss of Reputation or Business
- Requirement to notify all Customers
- As well as the ability to accept major payment cards

PCI Compliance Team

- Scott Bennett, Associate VP, Administration & Finance
- Robert Berry, Director, Internal Auditing Office
- Joann Campbell, Associate VP Compliance Officer, President's Office
- Jeff Durfee, Director, Networking, Systems & Security
- Mike Neglia, Treasurer, Treasury Office
- Valerie Stevenson, Controller, Controller's Office

For Help with PCI Compliance Issues contact:

- Treasury Department: treasury@unf.edu
- ITS Security: ITSecurity@unf.edu <or> Submit an ITSR
- Controller's Office: controlr@unf.edu

Video Presentation

http://youtu.be/xpfCr4By71U

http://www.youtube.com/watch?v=xpfCr4By71U&feature=player_embedded

Link for Assessment

http://tinyurl.com/UNF-PCI

Password: {contact Angela Lee}

Score 10/10 ~ You're a PCI Compliance Guru

Score 9/10 ~ You're a PCI Compliance Whiz

Score 8/10 ~ You're PCI Compliance Green

You *must* Retake Assessment if you score less than 8/10 correct. Thank you!

Scores & Annual Renewal

Scores and Dates of Assessment will be retained by the Controller's Office to fulfill compliance procedures. If you have any questions please e-mail: controlr@unf.edu

Questions and Thank you for attending

Angela Lee, Training Coordinator for the Division of Administration & Finance, **alee@unf.edu** or **620-2950**