

**Payment Card Industry (PCI)  
Data Security Standards**

Information Privacy and Security  
(IPAS) Project

Mike Leach, Project Manager  
Jenn Stewart, Technical Coordinator

---

---

---

---

---

---

---

---

**Heartland Payment Systems – January 2009**

- \* 100 million transactions per month
- \* Unclear how many account numbers were compromised
- \* Visa and MasterCard alerted of suspicious activity
  - Malicious software crossed the network
- \* Associated costs:
  - Became a level 1 merchant (more on this later)
  - Outside forensics investigators
  - Lawsuits occur
  - May be largest data breach in U.S. history

---

---

---

---

---

---

---

---

**Pennsylvania State University-?**

- Compromises involving credit cards have occurred
- Fines have been assessed on merchants
- Remediation efforts are long term (~year)
- Department was/is responsible for all costs and remediation efforts

*Learning Tip:*  
*[Don't drill holes in your end of the boat]*

---

---

---

---

---

---

---

---

### Learning Objectives for Today

- Introduce the Payment Card Industry Data Security Standards (PCI DSS)
- Review Penn State's approach
- Understand the Reference Architecture
- Identify your role, IPAS role
- Maintain a compliant environment
- Prepare for PCI assessments
- Open dialog/information sharing

---

---

---

---

---

---

---

---

### The "Council"



- Payment Card Industry Security Standards Council (PCI SSC or the Council)
- Open, global forum
- Five card brands, founded 2006
- Responsible for PCI Security Standards
  - Development
  - Management
  - Education

PCI SSC Founders



Participating Organizations  
Merchants, banks, processors, developers and point of sale vendors

---

---

---

---

---

---

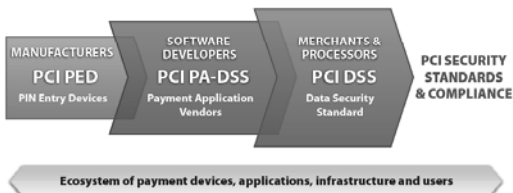
---

---

### The Standards, yes with an "s"

#### PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



---

---

---

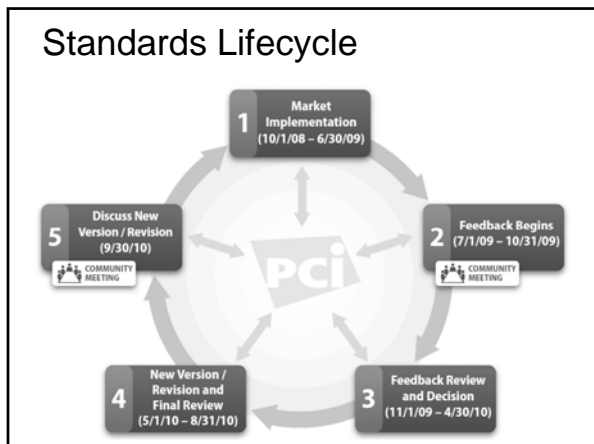
---

---

---

---

---



---

---

---

---

---

---

---

---

### What is considered "IN SCOPE"?

- CPE includes any device or terminal that:
  - Processes credit cards
  - Transmits credit card information
  - Stores credit card information
- Device or terminal in CPE
  - Point of Sale terminal (POS)
  - Computer terminal, server
  - IDS/IPS
  - Firewall, switch

---

---

---

---

---

---

---

---

### Penn State's Approach to PCI DSS

---

---

---

---

---

---

---

---

**Designated Contacts Responsibilities**

- Financial and Administrative Contacts**
- Work to identify costs and secure funding
  - Provides leadership for the project
  - Interface with Budget Executive
- Technical Contact**
- Coordinates and implements required security improvements
- Administrative Contact**
- Also responsible for developing policies and procedures

---

---

---

---

---

---

---

---

---

---

**Credit Card Processing Options**

- Penn State eCommerce
  - ePay
  - PSU Pay
  - eStore
  - PSU Checkout
- Point of Sale Devices (POS)
- Third Party Applications
- Review Penn State Guru Policy
  - FN 07, Credit Card Sales

---

---

---

---

---

---

---

---

---

---

**Acceptable Entry on PSU Computer**

	ePay	POS	eStore	PSU Pay
Phone	Y	Y	N	N
Fax	Y	Y	N	N
Mail	Y	Y	N	N
In-Person	Y	Y	N	N

---

---

---

---

---

---

---

---

---

---

PCI DSS  
Requirements

---

---

---

---

---

---

---

---

PCI DSS Control Objectives

Each objective consists of at least one requirement

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Vulnerability Management
4. Implement Strong Access Controls
5. Regularly Monitor and Test
6. Maintain an Information Security Policy

---

---

---

---

---

---

---

---

PCI DSS Requirement 1

*1. Configure firewall to protect cardholder data*

- Must be hardware appliances
- Inbound and outbound connections by exception ONLY
- Firewall rule-set review every six months
- Requires NAT on internal addresses
- Update network diagrams with changes

---

---

---

---

---

---

---

---

## PCI DSS Requirement 2

### 2: Eliminate vendor default credentials

- Hardware: switches, computers, servers, etc
- Software: operating systems, applications
- Comply with role-based security policies
  - SANS, NIST, CIS provide good guidelines
- Server function: one per machine
- Remove unnecessary services, protocols

---

---

---

---

---

---

---

---

## PCI DSS Requirement 3

### 3. Protect stored cardholder data

- Keep data storage to a minimum:
  - Obscure the PAN
    - The first six and last four are permissible
- Don't store authentication data
  - Recognize the difference between transaction and authentication data
- Protect encryption keys

---

---

---

---

---

---

---

---

## Data Elements Chart

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
<b>Cardholder Data</b>	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
<b>Sensitive Authentication Data**</b>	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

---

---

---

---

---

---

---

---

Use Your Knowledge: Answer this Scenario

It is acceptable to store a combination of:

1234 56xx xxxx 3456  
+  
name  
+  
expiry data together?

---

---

---

---

---

---

---

---

PCI DSS Requirement 4

4. *Encrypt transmission of cardholder data*

- Strong encryption
  - Minimum 128 bit keys – Synchronous cryptography
  - Minimum 2048 bit keys – Public / Private keys
- Effective protocols (SSL/TLS and IPSec)
- Wireless is not recommended
- NEVER send PANs via email

---

---

---

---

---

---

---

---

PCI DSS Requirement 5

5. *Use anti-virus software*

- All systems require anti-virus software
- Keep signature files current and updated
- Generate audit logs
  - Send separate server
  - Retain at least 1 year
    - Minimum of 3 months online

---

---

---

---

---

---

---

---

PCI DSS Requirement 6

6. *Keep systems and applications secure*

- Employ a patching scheme
- Identify new vulnerabilities
- Install critical system and device patches within one month of release and lower priority within at least three months
- Separate production and test environments
  - Eliminate test data on the production network

---

---

---

---

---

---

---

---

PCI DSS Requirement 6

6. *Keep systems and applications secure (cont'd)*

- Define and adhere to change control procedures
- Application code review or application firewall
- Third-party vendors
  - Must comply with the PA DSS (Payment Application Data Security Standards)
  - Phased application of standards through 2009

---

---

---

---

---

---

---

---

PCI DSS Breather

Summary of Req. 1-6

1. Firewall
2. No default credentials
3. Encrypt stored data
4. Encrypt transmitted data
5. Use antivirus software
6. Harden systems and applications

---

---

---

---

---

---

---

---

PCI DSS Requirement 7

7. Restrict access to cardholder data

Business need-to-know

- Restrict data access to authorized personnel only
- Audit system access

---

---

---

---

---

---

---

---

PCI DSS Requirement 8

8. Enforce access accounting

- Users must have unique digital identity
  - Require one factor authentication
  - Group passwords are prohibited
- Remote access requires two-factor authentication
  - Must be secured with strong encryption
- Require re-authentication after 15-minute session idle

---

---

---

---

---

---

---

---

PCI DSS Requirement 8

8. Enforce access accounting (cont'd)

- Identity verification prior to password resets
- Account revocation of terminated employees
- Strong passwords
  - Change every 90 days, minimum
  - At least 8 characters long
  - Combination of alphabetic and numeric characters

---

---

---

---

---

---

---

---

### PCI DSS Requirement 9

*9. Restrict physical access to cardholder data*

- Enforce secure access where cardholder data is stored:
  - Install cameras in data centers
  - Require authorization prior to entering
  - Document and supervise visitors (badge, log retention)
- Destroy paper and electronic media immediately after use

---

---

---

---

---

---

---

---

### PCI DSS Requirement 10

*10. Track and monitor all access to network resources and cardholder data*

- Logging is required for:
  - User access to any cardholder data
  - Access to everything from administrator or root account
  - Login attempts, both success and failure
- Synchronize system clocks
- Secure logs so they cannot be modified
  - Maintain three months online and one year offline
  - Monitor file integrity

---

---

---

---

---

---

---

---

### PCI DSS Requirement 11

*11. Regularly test security systems and processes*

- Annual penetration tests
  - Network and applications
  - Physical security
- Internal and external scans
- Host-based and/or network-based intrusion detection
- Run wireless analyzer at least quarterly
- Monitor file integrity

---

---

---

---

---

---

---

---

**PCI DSS Requirement 12**

*12. Maintain an Information Security policy*

- Address all PCI DSS objectives
- Annual process to identify threats & vulnerabilities
- Define assigned job roles
  - Create training modules that cover policies and procedures for CPE
- Incident response plan
  - Contact SOS

---

---

---

---

---

---

---

---

**PCI DSS Breather**

Summary of Req. 7-12

- 7. Restrict access, need-to-know
- 8. Enforce access accounting
- 9. Physical restrictions
- 10. Monitor resources and data
- 11. Test systems and processes
- 12. Maintain an information security policy

---

---

---

---

---

---

---

---

**Prohibited Uses**

Never email CHD. If received in email from customer:

1. Remove the CHD from the email
2. Respond to the customer that they must register or purchase the item through the designated online application or call to provide their CHD
3. Delete the original email with the CHD
4. Clear the deleted items from the recycle bin

---

---

---

---

---

---

---

---

**Paper Storage Best Practices**

- Enter CHD immediately
  1. Black out CHD on the original
  2. Copy the original
  3. Shred the original
  4. File the copy
- Use transaction number to reference
- Secure fax machines
- Reduce scope

---

---

---

---

---

---

---

---

**Reference  
Architecture**

---

---

---

---

---

---

---

---

**CPE Network**

- Separate workstations from department LAN
- Protect the CPE with a hardware firewall.
  - May be alternate interface on an existing firewall
- Enable logging and store on a protected logging server
  - User logs, workstation logs, firewall logs, and network logs
- Enable encryption throughout process

---

---

---

---

---

---

---

---

User Restrictions

- Individual logins and strong passwords
- Restrict privilege that allows users to alter the system or load software
- Only allow users who have a "need to know" and follow PCI DSS
- Users are not permitted to use ANY form of Internet based instant messaging
- Internet or Web surfing must be limited to "business only" use

---

---

---

---

---

---

---

---

CPE Workstations

- Remove unnecessary local accounts
- Disable boot from CD/DVD drive, USB ports
- Disable any unnecessary services
- Install only "business need" applications and keep patches current
- Enable a personal firewall
- Lock down terminal to only essential applications
- Keep anti-virus and anti-spyware/malware current
- Keep operating system current
- Install and utilize host based or network based IDS

---

---

---

---

---

---

---

---

Ongoing Process

---

---

---

---

---

---

---

---

### Annual Self Assessment Questionnaire

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone order) merchants; all cardholder data functions outsourced. This would never apply to face-to-face merchants.	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone terminal merchants, no electronic cardholder data storage	B
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (no included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ	D

---

---

---

---

---

---

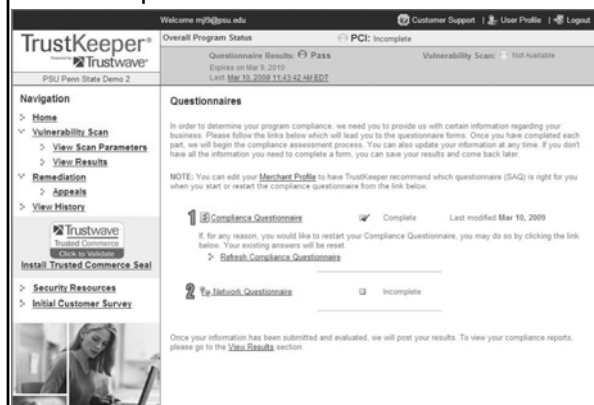
---

---

---

---

### TrustKeeper Unit Portal




---

---

---

---

---

---

---

---

---

---

### Responsibilities

#### Merchant

- Maintain secure Card Processing Environment (CPE)
  - Notify IPAS of infrastructure changes
  - Purchase, install, maintain new equipment
- Renew SAQ annually
- Request quarterly scans (internal and external)

#### IPAS Project Team

- Assist PSU merchants on compliance efforts (verbally)
- Conduct assessments
- Report to Corporate Controller
- Review third party contracts
- Manage admin side of TrustKeeper Portal
- Serve as liaison between QSA and University

---

---

---

---

---

---

---

---

---

---

# PCI Assessments

---

---

---

---

---

---

---

---

- ### Assessment Process
- Review technical aspects
    - Firewall rules
    - Input terminals
    - Logging
    - File Integrity Monitoring
    - Backup procedures
    - Wireless analyzer
    - Web apps
  - Review physical security

---

---

---

---

---

---

---

---

- ### Assessment Follow-up
- IPAS team will provide a summary of findings with recommendations
  - Response plan requested within two weeks
  - IPAS reviews plan
    - Reply with acceptance or suggestions/changes
    - Maintain an open dialogue
  - Follow-up until complete

---

---

---

---

---

---

---

---

### What are we finding?

- Firewalls not tight enough
  - Network not locked down
- Unsecured terminals
  - AV/OS patches out of date
- Logging not sufficient
  - Not using centralized server
  - No File Integrity Monitoring
- Shared accounts in use; expired accounts active
- Wireless analyzer not being used
- Policy and procedures not detailed enough

---

---

---

---

---

---

---

---

### Events Resulting from Compromise

- The burden of proof is difficult to achieve
  - Long term
  - Much paperwork
  - External parties involved
- The penalties in dollars, resources and your time are real
- Compromises are typically network based; this is why network protections are so stringent

---

---

---

---

---

---

---

---

### Resources

- IPAS Project Website
  - <http://ipas.psu.edu>
- PCI
  - <https://www.pcisecuritystandards.org>
- PCI DSS v1.1
  - [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download\\_agreement.html](https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html)
- SANS
  - <http://www.sans.org>
- CERT
  - <http://www.cert.org>
- ITS Training Services
  - <http://its.psu.edu/training>

---

---

---

---

---

---

---

---

### Contacts

#### IPAS Project Office

- Phone: 814-867-1340
- Email: IPAS@psu.edu
- Web: ipas.psu.edu

#### SOS

- 8:00-5:00 ...814-863-9533
- after hrs .... 814-777-9533
- Email: security@psu.edu
- Web: sos.its.psu.edu

#### Training Services

- Phone: 814-863-9522
- Email: ITSTraining@psu.edu
- Web: its.psu.edu/training

#### Privacy Office

- Phone: 814-863-3049
- Email: privacy@psu.edu
- Web: www.psu.edu/privacy

---

---

---

---

---

---

---

---

Information Sharing  
Open Dialog

---

---

---

---

---

---

---

---