


# PCI DSS 101 & 102




D.J. Vogel, CISSP, CISA  
403 Labs, LLC

## Agenda




- Background
- Responsibilities
- 12 Requirements

## Background




- Early 2000, Visa introduced security programs:
  - Cardholder Information Security Program (CISP) to the US
  - Account Information Security (AIS) Program to the EU
- Mandated compliance in 2001

## Background (cont.)




- MasterCard's Site Data Protection (SDP) program
- American Express's Data Security Operating Policy (DSOP)
- Discover Information Security and Compliance (DISC) program
- Diners Club and JCB followed

## Background (cont.)



- Each program had its own standards
- Differing validation requirements
- All had same goal:  
Protect cardholder data


## PCI DSS



- Lots of feedback from industry
- Visa and MasterCard developed the Payment Card Industry (PCI) Data Security Standard (DSS)
- Other card associations have also endorsed the Program

## PCI DSS (cont.)

- Officially announced January 2005
- Standard covers multiple associations
- Compliance with one global standard
- Single validation




## Agenda

- Background
- **Responsibilities**
- 12 Requirements



## Responsibilities

- Who Must Comply
- Merchant Levels
- Compliance Validation
- Validation Timeline
- Validation Procedures
- Benefits
- If Compromised
- Penalties



## Who Must Comply

- **ALL** merchants and service providers that:
  - Store
  - Process
  - Transmit
- **ALL** payment channels
  - Retail (brick-and-mortar)
  - Mail/telephone order
  - eCommerce




## Who Must Comply (cont.)

- Differing requirements for ecommerce merchants
- All merchants must be compliant
- NOT restricted to ecommerce




## Merchant Levels

- Three considerations:
  1. How many total annual transactions?
  2. How many e-commerce transactions?
  3. Have you been compromised before?




## Merchant Levels (cont.)

- Level 1
  - > 6M annual transactions,
  - Any organization that has had a compromise in the past,
  - or
  - Any merchant at the card associations' discretion




## Merchant Levels (cont.)

- Level 2
  - 150,000 – 6M annual **ecommerce** transactions
- Level 3
  - 20,000 – 150,000 annual **ecommerce** transactions




## Merchant Levels (cont.)

- Level 4
  - < 20,000 annual **ecommerce** transactions,
  - and
  - < 6M total annual transactions




## Compliance Validation

- Independent PCI validation
- Identify and correct vulnerabilities




## Validation Timeline

- Level 1 – September 30, 2004
- Level 2 – June 30, 2005
- Level 3 – June 30, 2005
- Level 4 – Acquirer's discretion



## Validation Procedures

- Level 1
  - Onsite Audit
  - Quarterly Network Security Scan
- Level 2, Level 3 and Level 4
  - Self-Assessment Questionnaire
  - Quarterly Network Security Scan



## Validation Procedures

- Onsite Audit
  - Can be performed by internal audit, dependent on acquirer
- Self-Assessment Questionnaire
  - Completed internally, but must address any system(s) that process, store or transmit cardholder data
- Quarterly Network Security Scan
  - Must be performed by Qualified Scan Vendor



## Benefits

- Competitive edge gained
- Increased revenue and improved bottom line
- Positive image maintained
- Customers are protected



## If Compromised

- IF compromise is suspected
- Report to your Merchant Bank
- Stringent timeline and defined responsibilities



## Penalties

- Noncompliance or failure to rectify issue
- If compromised, fines up to \$500,000 PER INCIDENT
  - Those compliant at the time of breach receive protection
- Additional fines may also be set



## Agenda

- Background
- Responsibilities
- **12 Requirements**




## 12 Requirements

- PCI DSS is organized into 12 requirements
- These 12 requirements fit nicely into 6 categories




**Category 1**

- **Build and Maintain a Secure Network**
  1. Install and maintain a firewall configuration to protect data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters




**Category 2**

- **Protect Cardholder Data**
  3. Protect Stored Data
  4. Encrypt transmission of cardholder data and sensitive information across public networks




**Category 3**

- **Maintain a Vulnerability Management Program**
  5. Use and regularly update anti-virus software
  6. Develop and maintain secure systems and applications




**Category 4**

- **Implement Strong Access Control Measures**
  7. Restrict access to data by business need-to-know
  8. Assign a unique ID to each person with computer access
  9. Restrict physical access to cardholder data




**Category 5**

- **Regularly Monitor and Test Networks**
  10. Track and monitor all access to network resources and cardholder data
  11. Regularly test security systems and processes



**Category 6**


- **Maintain an Information Security Policy**
  12. Maintain a policy that addresses information security



[

## Requirement 1

Install and maintain a firewall configuration to protect data




TRANSACTION SECURITY SUPPORT

[

## Req 1: Firewall

1.1 Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?




TRANSACTION SECURITY SUPPORT

[

## Req 1: Firewall

1.2 If wireless technology is used, is the access to the network limited to authorized devices?




TRANSACTION SECURITY SUPPORT

[

## Req 1: Firewall

1.3 Do changes to the firewall need authorization and are the changes logged?




TRANSACTION SECURITY SUPPORT

[

## Req 1: Firewall

1.4 Is a firewall used to protect the network and limit traffic to that which is required to conduct business?




TRANSACTION SECURITY SUPPORT

[

## Req 1: Firewall


1.5 Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?



TRANSACTION SECURITY SUPPORT


[ Req 1: Firewall ]

1.6 Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?




[ Req 1: Firewall ]

1.7 If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment?




[ Req 1: Firewall ]

1.8 Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?




[ Req 1: Firewall ]

1.9 Are Web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)?




[ Req 1: Firewall ]

1.10 Is the firewall configured to translate (hide) internal IP addresses, using network address translation (NAT)?




[ Requirement 2 ]

Do not use vendor-supplied defaults for system passwords and other security parameters




**Req 2: Defaults**

2.1 Are vendor default security settings changed on production systems before taking the system into production?




**Req 2: Defaults**

2.2 Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?




**Req 2: Defaults**

2.3 If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)?




**Req 2: Defaults**

2.4 If wireless technology is used, is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable?




**Req 2: Defaults**

2.5 Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?



**Req 2: Defaults**

2.6 Are secure, encrypted communications used for remote administration of production systems and applications?



[ Req 3: Stored Data ]


## Requirement 3

Protect stored data




[ Req 3: Stored Data ]

3.1 Is sensitive cardholder data securely disposed of when no longer needed?




[ Req 3: Stored Data ]

3.2 Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products?




[ Req 3: Stored Data ]

3.3 Is it prohibited to store the card-validation code (three-digit value printed on the signature panel of a card) in the database, log files, or point-of-sale products?




[ Req 3: Stored Data ]

3.4 Are all but the last four digits of the account number masked when displaying cardholder data?



[ Req 3: Stored Data ]

3.5 Are account numbers (in databases, logs, files, backup media, etc.) stored securely— for example, by means of encryption or truncation?



### Req 3: Stored Data

- 3.6 Are account numbers sanitized before being logged in the audit log?



### Requirement 4

Encrypt transmission of cardholder data and sensitive information across public networks



### Req 4: Encryption

- 4.1 Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?



### Req 4: Encryption

- 4.2 If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?



### Req 4: Encryption

- 4.3 If wireless technology is used, is the communication encrypted using Wi-Fi Protected Access (WPA), VPN, SSL at 128-bit, or WEP?



### Req 4: Encryption

- 4.4 If wireless technology is used, are WEP at 128-bit and additional encryption technologies in use, and are shared WEP keys rotated quarterly?



## Req 4: Encryption

- 4.5 Is encryption used in the transmission of account numbers via e-mail?



## Requirement 5

Use and regularly update anti-virus software



## Req 5: Antivirus

- 5.1 Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?



## Requirement 6

Develop and maintain secure systems and applications



## Req 6: Development

- 6.1 Are development, testing, and production systems updated with the latest security-related patches released by the vendors?



## Req 6: Development

- 6.2 Is the software and application development process based on an industry best practice and is information security included throughout the software development life cycle (SDLC) process?



### Req 6: Development

6.3 If production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage?



### Req 6: Development

6.4 Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?



### Req 6: Development

6.5 Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group ([www.owasp.org](http://www.owasp.org))) taken into account in the development of Web applications?



### Req 6: Development

6.6 When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?



### Req 6: Development

6.7 Is sensitive cardholder data stored in cookies secured or encrypted?




### Req 6: Development

6.8 Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?




[ Requirement 7 ]



Requirement 7


Restrict access to data by business need-to-know

[ Req 7: Restrict Access ]




7.1 Is access to payment card account numbers restricted for users on a need-to-know basis?

[ Req 8: User Accounts ]



8.1 Are all users required to authenticate using, at a minimum, a unique username and password?


[ Requirement 8 ]



Requirement 8


Assign a unique ID to each person with computer access

[ Req 8: User Accounts ]



8.2 If employees, administrators, or third parties access the network remotely, is remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on?

[ Req 8: User Accounts ]



8.3 Are all passwords on network devices and systems encrypted?

## Req 8: User Accounts

8.4 When an employee leaves the company, are that employee's user accounts and passwords immediately revoked?



## Req 8: User Accounts

8.5 Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?



## Req 8: User Accounts

8.6 Are non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system after a pre-defined period?



## Req 8: User Accounts

8.7 Are accounts used by vendors for remote maintenance enabled only during the time needed?



## Req 8: User Accounts

8.8 Are group, shared, or generic accounts and passwords prohibited for non-consumer users?



## Req 8: User Accounts

8.9 Are non-consumer users required to change their passwords on a pre-defined regular basis?



## Req 8: User Accounts

8.10 Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords?



## Req 8: User Accounts

8.11 Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?



## Requirement 9

Restrict physical access to cardholder data



## Req 9: Physical Access

9.1 Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?



## Req 9: Physical Access

9.2 If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices?




## Req 9: Physical Access

9.3 Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?




[ Req 9: Physical Access ]

9.4 Is all cardholder data printed on paper or received by fax protected against unauthorized access?




[ Req 9: Physical Access ]

9.5 Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?




[ Req 9: Physical Access ]

9.6 Are all media devices that store cardholder data properly inventoried and securely stored?



[ Req 9: Physical Access ]

9.7 Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?



[ Requirement 10 ]


**Requirement 10**

Track and monitor all access to network resources and cardholder data




[ Req 10: Logging ]

10.1 Is all access to cardholder data, including root/administration access, logged?




[ Req 10: Logging ]

10.2 Do access control logs contain successful and unsuccessful login attempts and access to audit logs?




[ Req 10: Logging ]

10.3 Are all critical system clocks and times synchronized, and do logs include date and time stamp?




[ Req 10: Logging ]

10.4 Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?



[ Req 10: Logging ]


10.5 Are audit logs regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems?



[ Requirement 11 ]


Requirement 11

Regularly test security systems and processes




[ Req 11: Testing ]

11.1 If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?




**Req 11: Testing**

11.2 Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?




**Req 11: Testing**

11.3 Is an intrusion detection or intrusion prevention system used on the network?




**Req 11: Testing**

11.4 Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored, and are the latest IDS/IPS signatures installed?




**Requirement 12**

Maintain a policy that addresses information security




**Req 12:**

12.1 Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?




**Req 12:**

12.2 Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?




[ Req 12: ]

12.3 Are information security policies reviewed at least once a year and updated as needed?




[ Req 12: ]

12.4 Have the roles and responsibilities for information security been clearly defined within the company?




[ Req 12: ]

12.5 Is there an up-to-date information security awareness and training program in place for all system users?




[ Req 12: ]

12.6 Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?




[ Req 12: ]

12.7 Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers?




[ Req 12: ]

12.8 Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?




[ Req 12: ]

12.9 Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?




[ Req 12: ]

12.10 Are security incidents reported to the person responsible for security investigation?



[ Req 12: ]

12.11 Is there an incident response team ready to be deployed in case of a cardholder data compromise?



[ Agenda ]

- Background
- Responsibilities
- 12 Requirements



[ Thank you! ]

D.J. Vogel, CISSP, CISA  
403 Labs, LLC  
[djvogel@403labs.com](mailto:djvogel@403labs.com)

[http://www.403labs.com/presentations/safe\\_pcidss.pdf](http://www.403labs.com/presentations/safe_pcidss.pdf)

