



# PCI Controls Self-Assessment

## PCI Controls Self-Assessment

### PCI/DSS Controls

#### *Six Objectives of PCI DSS*

1. Secure Networks via Firewall Implementation
2. Protect Cardholder Data
3. Establish a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly monitor and test networks
6. Maintain an information security policy.

#### **Objective #1: Secure Networks via Firewall Implementation**

Cardholder data refers to any information printed, processed, transmitted, or stored in any form on a payment card. Firewalls are one of the oldest computer security protections and are a mission-critical component for network defense. Because many aspects of data protection begin with firewalls, most of the Payment Card Industry Data Security Standard (PCI DSS) includes network firewall-related clauses. (PCI DSS 1 & 2)

#### **Key Control Requirements**

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

#### **Control Checklist**

- Reformat all default vendor-supplied passwords.
- Restrict both inbound and outbound traffic to your payment systems to only what is necessary.
- Avoid the use of "Any" in firewall allow rules.
- "Deny all" traffic that you do not specifically authorize.
- Permit only "established" connections into your network (for example, via stateful packet inspection or dynamic packet filtering).
- Turn on intrusion detection and intrusion blocking, if available.
- Turn on notifications.

- Turn on Network Address Translation (NAT) to hide your internal addresses from the Internet.
- Check for and install firewall updates (or patches) to address new vulnerabilities as soon as the patch is available.
- Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
- Develop and update configuration standards for all system components that address all known security vulnerabilities.
- Using strong cryptography, encrypt all non-console administrative access.
- Maintain an inventory of system components that are in scope for PCI DSS.
- Ensure that related security policies and operational procedures are documented, in use, and known to all.
- Shared hosting providers must protect each entity's hosted environment and cardholder data.

### **Pre-audit Validation**

- Does <Client> automatically test whenever firewall and configuration standards change?
- Are firewalls configured to identify all connections to cardholder data, including wireless?
- How often does <Client> IT / Administrators review and revise firewall configuration settings?
- Are all attempted access from untrusted networks or hosts denied?
- Does anyone within the public have access to your cardholder data?
- Does <Client> manage a "BYOD" policy, and if so, are firewalls and other security devices and policies in place?
- Does <Client> manage and distribute documented operational policies and guidelines for security and privacy?
- What is <Client>' Password Policy?
- Are web-based management tools and browsers encrypted?
- If <Client> uses a shared hosting, cloud, or colocation provider, are those providers PCI compliant?

## **Objective #2: Protect Cardholder Data**

Cardholder data refers to any information stored in any form on a payment card. Businesses accepting payment cards are expected to protect cardholder data and to prevent its unauthorized use – whether the data is printed or stored locally or transmitted over an internal or public network to a remote server or service provider.

(PCI DSS 3 & 4)

### **Key Control Requirements**

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

**Control Checklist**

- Limit cardholder data storage and retention time to that which is required for business and purge unneeded data at least quarterly.
- Do not store authentication data after authorization (even if it is encrypted).
- Mask PAN when displayed so that only authorized people with a legitimate business need can see more than the first six/last four digits.
- Render PAN unreadable anywhere it is stored.
- Implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.
- Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.
- Create and maintain a data retention and disposal policy.
- Encrypt CHD using industry-accepted algorithms and security keys.
- Limit CHD storage amount and retention time.
- Define processes for secure deletion of CHD when no longer needed.
- Develop a process to identify and securely delete CHD if it exceeds the defined retention.
- Store only data elements as required for business (avoid storing full contents of any track).
- Restrict access to cryptographic keys.

**Pre-audit Validation**

- Does <Client>’ retention policy adhere to business, legal, and regulatory requirements?
- Is the data retention policy under periodic review by Counsel?
- Does <Client> discard / destroy / remove all authentication data after authorization and use?
- Does <Client> implement strong encryption on primary account numbers on all media, logs, and stored data?
- How does <Client> protect cryptographic keys?
- Does <Client> have proof of key management, including required sign-off?
- How does <Client> validate that only authorized personnel have access to full cardholder account numbers?
- Does <Client> implement strong cryptography or security protocols during open network transmissions?
- In accordance with PCI requirements, has <Client> discontinued using WEP?
- Does <Client> restrict employees from sending PANs or card data by email or instant messaging technology?

### Objective #3: **Establish a Vulnerability Management Program**

Vulnerability management is the process of finding weaknesses in a business' payment card system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

(PCI DSS 5 & 6)

#### Key Control **Requirements**

5. Protect all systems against malware and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.

#### Control **Checklist**

- Deploy anti-virus software on all systems commonly affected by malicious software.
- Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs.
- Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.
- Define and implement a development process that comprises security requirements in all stages of the development.
- Install critical security patches.
- Ensure the test environment is kept separate.
- Review custom code before release to production or customers.

#### Pre-audit **Validation**

- Does <Client> deploy antivirus/antimalware on all systems that could potentially contract hostile code, including mobile devices, computers, and servers?
- Are all security applications current and properly licensed?
- Are audit logs available for review?
- How does <Client> validate that all antivirus / antimalware tools are continuously running?
- Does <Client> perform a periodic audit to ensure critical patches have been installed? (Scheduled when & how often)
- Does <Client> or its MSP subscribe to alert services for your software applications?
- Does <Client> use a vulnerability scanning service?
- Does that vulnerability scanning service amend as needed for configuration modifications?
- Which common cybersecurity framework does <Client> follow?
- How does <Client> identify developing vulnerabilities when systems or configurations are updated?
- Does <Client> review public-facing web applications on an annual basis?
- Does <Client> implement a Web Application Firewall?

**Objective #4: Implement Strong Access Control Measures**

Access-controls allow businesses to permit or deny access to PAN and other cardholder data. Access must be granted on a business need-to-know basis. Physical access controls entail the use of locks or other means to restrict access to computer media, paper-based records, or system hardware. Logical access controls permit or deny use of payment devices, wireless networks, PCs and other computing devices, and also controls access to digital files containing cardholder data.

(PCI DSS 7, 8 & 9)

**Key Control Requirements**

7. Restrict access to cardholder data by business need to know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.

**Control Checklist**

- Define and implement a development process that comprises security requirements in all stages of the development.
- Install critical security patches.
- Ensure the test environment is kept separate.
- Review custom code before release to production or customers .
- Define and implement a development process that comprises security requirements in all stages of the development.
- Install critical security patches.
- Ensure the test environment is kept separate.
- Review custom code before release to production or customers.
- Define and implement a development process that comprises security requirements in all stages of the development.
- Install critical security patches.
- Ensure the test environment is kept separate.
- Review custom code before release to production or customers.

**Pre-audit Validation**

- Can any employee access card data or systems who does not have card processing in their job description?
- Does <Client> ' access control system incorporate multiple levels of access, based on "Principle of Least Privilege"?
- Are unauthorized requests for access automatically denied?
- Do all <Client> employees maintain a unique ID?
- Does <Client> require password access into its systems?
- Are all stored passwords encrypted?
- Is transmission of passwords encrypted?
- Does <Client> require two-factor authentication for remote access?
- Does <Client> ' virtual private network (VPN) include individual certificates?
- Are restrictions in place for specific users?

- ✎ Do <Client> System Admins have proper access where required?
- ✎ Is <Client> ' cardholder data environment limited from access by the public or other unauthorized users?
- ✎ Does <Client> maintain secured / off-site data backups?
- ✎ Are all paper copies of cardholder data secured with a lock?

### **Objective #5: Regularly Monitor / Test Networks**

Physical and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment card applications and cardholder data. To prevent exploitation, organizations must regularly monitor and test networks to find and fix vulnerabilities.

(PCI DSS 10 & 11)

#### **Key Control Requirements**

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

#### **Control Checklist**

- Document how data flows into your organization
- Implement audit trails for all user log in, unsuccessful login attempts, and changes such as creation and deletion of system-level objects
- Limit view of audit trails
- Review all security events and logs of all system components (that handle CHD), critical system components, and servers that perform security functions, such as firewalls, intrusion prevention systems, authentication servers, and more
- Conduct internal vulnerability scan quarterly
- Conduct application penetration and network penetration tests on all external domains & IPs every year
- Conduct a quarterly wireless analyzer scan to discover all authorized as well as unauthorized wireless access points
- Scan external IPs and domains by a PCI-Approved Scanning Vendor (ASV)

#### **Pre-audit Validation**

- ✎ Is access to systems easy to connect to unique user IDs?
- ✎ Can <Client> System Administrators automatically identify access to cardholder data by user ID?
- ✎ Can <Client> automatically identify all administrative activities by user ID?
- ✎ Can <Client> systems identify invalid access attempts by user ID?
- ✎ Does <Client> systems generate audit logs?
- ✎ Can <Client> systems track user identification, activities, time stamps and point of origination?

- Are <Client> system locks synchronized?
- Are <Client> administrative users limited on how to modify audit trails?
- How often are security logs reviewed?
- Does <Client> retain audits for at least 12 months?
- Can <Client> identify all wireless access points?
- Does <Client> perform vulnerability scans every three months or more?  
(If so / not, how often?)
- Does <Client> conduct vulnerability scans following any changes to its network?
- Does <Client> perform penetration testing on an annual basis?
- Does <Client> automatically monitor all traffic in your cardholder data environment?
- Does <Client> receive immediate notification of any unusual traffic patterns?
- Does <Client> have the ability to perform critical file comparisons at least once a week, using file integrity monitoring software?

### **Objective #6: Establish / Manage an Information Security Policy**

A strong security policy sets the tone for security affecting an organization's entire company, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

(PCI DSS 12)

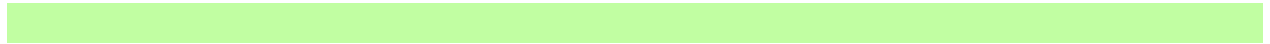
#### **Key Control Requirement**

12. Maintain a policy that addresses information security for all personnel.

#### **Control Checklist**

- Establish, publish, maintain, and disseminate a security policy and review the security policy at least annually and update when the environment changes.
- (Drew advises using the NIST CSF as a policy standard).
- Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email, and Internet.
- Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.
- Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.
- Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.
- Conduct user awareness training.
- Implement an incident response plan.
- Evaluate risks to identify essential assets, vulnerabilities, and threats.
- Run employee background checks.

### ***Pre-audit Validation***

- Does <Client> maintain an active security policy that addresses all PCI requirements?
  - Is that security policy reviewed and updated on an annual basis or more often?
  - How often is the security policy updated and under what conditions?
  - Does <Client> have an acceptable use policy for all employees and contractors?
  - Does the acceptable use policy address remote access, wireless connections, removable electronic media, laptops, handheld devices, email, and internet usage?
  - Does <Client> publish an in-house Employee Handbook, and if so, does that handbook declare the responsibility of every employee to protect card data?
  - Does <Client> employ / contract a designated Information Security Professional?
  - Are <Client> employees trained on security best practices?
  - Are background checks performed prior to hire?
  - Does <Client> validate all service providers to be compliant with PCI?
  - Can <Client> respond immediately to a system breach?
  - How often does <Client> test its incident response plan and when was the last test conducted?
- 

### **Compensating Controls Clause**

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of compensating controls.

For a compensating control to be considered valid, it must be reviewed by an assessor. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control.

Boulevard labs should be aware that a particular compensating control will not be effective in all environments.

➔ *Reference PCI DSS Appendices B and C for further details.*