

PCI Module Introduction

Department Contact Information

Field	Answer
Corporate Name	
DBA(s)	
Phone	
Contact Name	
Title	
Email	
Approximate # of Transactions/Accounts handled per year	
Please include a brief description of your business	
Processor	
Web Hosting	
Co-Location	
List Point of Sale (POS) software and hardware in use	
Gateway	
Shopping Cart	
Other	

PCI Standard: *Implement policies and procedures to install and maintain a firewall configuration to protect data.*

1.1) Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards? Yes No

PCI Standard: Implement policies and procedures to install and maintain a firewall configuration to protect data.

1.1) Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards? Yes No

1.2) If wireless technology is used, is the access to the network limited to authorized devices? If N/A please specify (250 char max.) Yes No NA

1.3) Do changes to the firewall need authorization and are the changes logged? Yes No

1.4) Is a firewall used to protect the network and limit traffic to that which is required to conduct business? Yes No

1.5) Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses? Yes No

1.6) Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by firewall? Yes No

1.7) If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment? If N/A please specify (250 char max.) Yes No NA

1.8) Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed? If N/A please specify (250 char max.) Yes No NA

1.9) Are web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)? Yes No

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

Yes No

PCI Standard: Implement policies and procedures to avoid usage of vendor-supplied defaults for system passwords and other security parameters.

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

Yes No

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

Yes No

2.3) If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)? If N/A please specify (250 char max.)

Yes No NA

2.4) If wireless technology is used is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable? If N/A please specify (250 char max.)

Yes No NA

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

Yes No

2.6) Are secure, encrypted communications used for remote administration of production systems and applications? If N/A please specify (250 char max.)

Yes No NA

PCI Standard: Implement policies and procedures for protection of Stored Data.

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

Yes No

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 base, log files, or point-of-sale products?

Yes No

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?

Yes No

3.4) Are all but the last four digits of the account number masked when displaying cardholder data?	Yes	No
3.5) Are account numbers (in databases, logs, files, backup media, etc.) stored securely for example, by means of encryption or truncation?	Yes	No
3.6) Are account numbers sanitized before being logged in the audit log?	Yes	No
3.7) Is there a documented data retention and disposal policy which specifies data retaining and storing procedures?	Yes	No
3.8) Are encryption keys used for the encryption of cardholder data safeguarded against disclosure and misuse?	Yes	No
3.9) Is there a documented data retention and disposal policy which specifies data retaining and storing procedures?	Yes	No

PCI Standard: Implement policies and procedures for encrypted transmission of cardholder data and sensitive information across public networks.

4.1) Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?	Yes	No	
4.2) If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption? If N/A please specify (250 char max.)	Yes	No	NA
4.3) If wireless technology is used, is the communication encrypted using Wi-Fi Protected Access (WPA), LEAP, VPN, SSL at 128-bit, or WEP? If N/A please specify (250 char max.)	Yes	No	NA
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? If N/A please specify (250 char max.)	Yes	No	NA
4.5) Is encryption used in the transmission of account numbers via e-mail? If N/A please specify (250 char max.)	Yes	No	NA

PCI Standard: Implement policies and procedures to regularly use and update anti-virus software.

5.1 Do virus susceptible machines have anti-virus software installed?	Yes	No	
5.2) Are installed anti-virus mechanisms current, actively running, and capable of generating audit logs? If N/A please specify (250 char max.)	Yes	No	NA

PCI Standard: Implement policies and procedures to develop and maintain secure systems and applications.

	Yes	No	
6.1) Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	Yes	No	
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? If N/A please specify (250 char max.)	Yes	No	NA
6.3) If the production data is used for testing and development purposes, is sensitive cardholder data sanitized before usage? If N/A please specify (250 char max.)	Yes	No	NA
6.4) Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?	Yes	No	
6.5) Were the guidelines commonly accepted by the security community (such as Open Web Applications Security Project group (www.owasp.org)) taken into account in the development of Web applications? If N/A please specify (250 char max.)	Yes	No	NA
6.6) When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts? If N/A please specify (250 char max.)	Yes	No	NA
6.7) Is sensitivity cardholder data stored in cookies secured or encrypted? If N/A please specify (250 char max.)	Yes	No	NA
6.8) Are controls implemented on the server side to prevent SQL injections and other bypassing of client side-input controls? If N/A please specify (250 char max.)	Yes	No	NA

6.9) Is the application protected by a layer firewall or routinely reviewed by an entity which specializes in application security? Yes No

PCI Standard: Implement policies and procedures to restrict access to data by business need-to-know

7.1) Is access to payment card account numbers restricted for users on a need-to-know basis? Yes No

PCI Standard: Implement policies and procedures to assign a unique ID to each person with computer access.

8.1) Are all users required to authenticate using, at a minimum, a unique username and password? Yes No

8.2) If employees, administrators, or third parties access the network remotely, is remote access software (such as PC Anywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on? If N/A please specify (250 char max.) Yes No NA

8.3) Are all passwords on network devices and systems encrypted? Yes No

8.4) When an employee leaves the company, are that employee's user accounts and passwords immediately revoked? Yes No

8.5) Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist? Yes No

8.6) Are accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system at least every 90 days? Yes No

8.7) Are users required to change their passwords at least every 90 days? If N/A please specify (250 char max.) Yes No NA

8.8) Are group, shared, or generic accounts and passwords prohibited for non-consumer users? Yes No

8.9) Are non-consumer users required to change their passwords on a predefined regular basis? Yes No

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? Yes No

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? Yes No

PCI Standard: Restricting physical access to cardholder data.

9.1) Are there multiple physical security controls (such as badges, escorts, or cameras) in place that would prevent unauthorized individuals from gaining access to the facility? Yes No

9.2) If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices? If N/A please specify (250 char max.) Yes No NA

9.3) Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access? Yes No

9.4) Is all cardholder data printed on paper or received by fax protected against unauthorized access? Yes No

9.5) Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data? Yes No

9.6) Are all media devices that store cardholder data properly inventoried and securely stored? Yes No

9.7) Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)? Yes No

9.8) Are procedures in place that ensure management approves any and all media that is moved from a secured area? Yes No

9.9) Is a visitor log maintained as a physical audit trail of visitor activity? Yes No

PCI Standard: Regularly Monitor and Test Networks.

10.1) Is all access to cardholder data, including root/administration access, logged?	Yes	No
10.2) Do access control logs contain successful and unsuccessful login attempts and access to audit logs?	Yes	No
10.3) Are all critical system clocks and times synchronized, and do logs include date and time stamp?	Yes	No
10.4) Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?	Yes	No
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?	Yes	No

PCI Standard: Regularly test security systems and processes.

11.1) If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?	Yes	No
11.2) Are penetration test (i.e., network-layer and application-layer test) performed at least once per year and after any significant infrastructure or application upgrade?	Yes	No
11.3) Is an intrusion detection or intrusion prevention system used on the network?	Yes	No
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?	Yes	No
11.5) Are security controls, limitations, network connections, and restrictions annually tested?	Yes	No
11.6) Are internal and external network vulnerability scans ran at least quarterly?	Yes	No

PCI Standard: Maintain a policy that addresses information security.

12.1) Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	Yes	No
12.2) Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	Yes	No
12.3) Are information security policies reviewed at least once a year and updated as needed?	Yes	No
12.4) Have the roles and responsibilities for information security been clearly defined within the company?	Yes	No
12.5) Is there an up-to-date information security awareness and training program in place for all system users?	Yes	No
12.6) Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	Yes	No
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?	Yes	No
12.8) Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	Yes	No
12.9) Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	Yes	No
12.10) Are security incidents reported to the person responsible for security investigation?	Yes	No
12.11) Is there an incident response team ready to be deployed in case of a cardholder data compromise?	Yes	No