

# Self-Assessment Questionnaire D-PSP and Attestation of Compliance

Document No: 2744d82e-8fd6-4c24-a532-0d5b7452d471

---

## All other SAQ-Eligible Merchants and Service Providers

Version 3.1

April 2015



**Part 1. Service Provider and Qualified Security Assessor Information**

**1a. Service Provider Organization Information**

Company Name:	Class One - Hotel Oleander	DBA(S):	Class One - Hotel Oleander
Contact Name:	Javier Sabariz Cancio	Title:	
Telephone:		E-mail:	javiersabariz@classone.es
Business Address:		City:	
State/Province:		Country:	
ZIP:			
URL:			
ISA Name(s) (if applicable)			

**Part 1b. Qualified Security Assessor Company Information (if applicable)**

Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		E-mail:	
Business Address:		City:	
State/Province:		Country:	
ZIP:			
URL:			

## Part 2. Executive Summary

### Part2a. Scope Verification

#### Services that were INCLUDED in the scope of PCI DSS Assessment (check all that apply)

Name of service(s) assessed: Seven Stars (PMS)

Type of service(s) assessed:

Hosting Provider:	Managed Services (specify):	Payment Processing:
<input checked="" type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other hosting (specify)	<input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> PhysicalSecurity <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify)	<input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify)
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway / Switch
<input checked="" type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> MerchantServices	<input type="checkbox"/> Tax / Governments Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others."

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

#### Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):

Name of service(s) not assessed

Type of service(s) not assessed

Hosting Provider:	Managed Services (specify):	Payment Processing:
<input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / network <input type="checkbox"/> Physical space (co-location)	<input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> PhysicalSecurity <input type="checkbox"/> Terminal Management System	<input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call center <input type="checkbox"/> ATM

<input type="checkbox"/> Storage	<input type="checkbox"/> Other services (specify)	<input type="checkbox"/> Other processing (specify)
<input type="checkbox"/> Web		
<input type="checkbox"/> Security services		
<input type="checkbox"/> 3-D Secure Hosting Provider		
<input type="checkbox"/> Shared Hosting Provider		
<input type="checkbox"/> Other hosting (specify)		
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway / Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> MerchantServices	<input type="checkbox"/> Tax / Governments Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

Provide a brief explanation why any checked services were not included in the assessment:

### Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?	To charge the bookings when they are not refundable
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	No cardholder data is stored

### Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centres, call centres, etc.) and a summary of locations included in the PCI DSS review.

Type of facility: **Hotel** Number of facilities: **1** Location of facility: **Platja de Palma, Balears, Spain**

### Part 2d. Payment Application

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is Application PA-DSS Listed	PA-DSS Listing Expiry

### Part 2e. Description of environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- Connections into and out of the cardholder data environment (CDE).
- Critical system components within CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, if applicable.

Linux

Does your business use network segmentation to affect the scope of your PCI DSS environment?  Yes  No

(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

**Part 2f. Third-Party Service Providers**

Does your company share cardholder data with any third-party service (for example, gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking

Yes

No

**If yes:**

Name of service provider:	Description of services provided:

**Note:** Requirement 12.8 applies to all entities in this list.

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full - The requirement and all sub-requirements were assessed for that Requirement, and not sub-requirements were marked as "Not Tested" or "Not applicable" in the SAQ.
- Partial - One or more sub-requirements of the Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ.
- None - All sub-requirements of that Requirement were marked as "Not Tested" and/or "Not Applicable" in the SAQ. For all requirements identified as either "Partial" or "None", provide details in "Justification for Approach" column, including:
  - Details of specific sub-requirements that were marked as either "Not Tested" and/or "Not Applicable" in the SAQ.
  - Reason why sub-requirement(s) were not tested or not applicable.

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI DSS website.

Name of service assessed:

PCI DSS Requirement	Details of Requirements Assessed			Justification for approach (Required for all "Partial" or "None" responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 2:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 3:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 4:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 9:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Section 2: Self-Assessment Questionnaire D-PSP

This Attestation of Compliance reflects the results of a self-assessment, which is documented in the accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	08-10-2015
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ as being not applicable (N/A)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ as being not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

**Part 3. PCI DSS Validation**

Based on the results noted in the SAQ D-PSP dated 08-10-2015 8:27, Class One - Hotel Oleander asserts the following compliance status (check one):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI SAQ are complete, and all questions answered “yes”, resulting in an overall <b>COMPLIANT</b> rating, thereby Class One - Hotel Oleander has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI SAQ are complete, or some questions are answered “no,” resulting in an overall <b>NON-COMPLIANT</b> rating, thereby Class One - Hotel Oleander has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date for Compliance:</b></p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b>; One or more requirements are marked as "No" due to legal restriction that prevents requirement from being met. This option requires additional review from acquirer or payment board.</p> <p>If checked, complete the following:</p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 30%;">Affected requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected requirement	Details of how legal constraint prevents requirement being met				
Affected requirement	Details of how legal constraint prevents requirement being met						



### Part 3a. Acknowledgment of Status

**Service Provider confirms:**

<input checked="" type="checkbox"/>	Self-Assessment Questionnaire D-PSP, Version 3.1, April 2015 was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment.
<input checked="" type="checkbox"/>	I have confirmed with my payment vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize that I must reassess my environment and implement any additional PCI DSS requirements that apply.
<input checked="" type="checkbox"/>	No evidence of full track data(1), CAV2, CVC2, CID or CVV2 data(2), or PIN data(3) storage after transaction authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SCC Approved Scanning Vendor

### Part 3b. Service Provider Acknowledgement

Signature of Service Provider Executive Officer:		Date:	08-10-2015 08:54
Service Provider Executive Officer Name:	Vicente Rodriguez	Title:	director
Service Provider Company Represented:	Class One - Hotel Oleander		

### Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:			
Signature of QSA:		Date:	08-10-2015 08:54
QSA Name		QSA Company:	

### Part 3d. ISA Acknowledgement (if applicable)

If a ISA was involved or assisted with this assessment, describe the role performed:			
Signature of ISA:		Date:	08-10-2015 08:54
ISA Name		Title:	

#### Part 4. Action plan for Non-Compliant Status

Select the appropriate response for "Compliant to PCI DSS Requirement" for each requirement. If you answer "No" to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement

*Check with the applicable payment brand(s) before completing Part 4.*

PCI DSS Requirement	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (if Compliance Status is "NO")
1	Install and maintain a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
3	Protect stored cardholder data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
5	Use and regularly update anti-virus software or programs	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
8	Assign a unique ID to each person with computer access	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	



## Self-Assessment Questionnaire D-PSP

### Build and Maintain a Secure Network and Systems

#### Requirement 1: Install and maintain a firewall configuration to protect data

PCI DSS Question		Response:
1.1	Are firewall and router configuration standards established and implemented to include the following:	
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	Yes
1.1.2a	Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	Yes
1.1.2b	Is there a process to ensure the diagram is kept current?	Yes
1.1.3a	Is there a current diagram that shows all cardholder data flows across systems and networks?	Yes
1.1.3b	Is there a process to ensure the diagram is kept current?	Yes
1.1.4a	Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	Yes
1.1.4b	Is the current network diagram consistent with the firewall configuration standards?	Yes
1.1.5	Are groups, roles, and responsibilities for logical management of network components assigned and documented in the firewall and router configuration standards?	Yes
1.1.6a	Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification (for example, hypertext transfer protocol (HTTP), Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols)?	Yes
1.1.6b	Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?  <b>Note: Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.</b>	Yes
1.1.7a	Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?	Yes
1.1.7b	Are firewall and router rule sets reviewed at least every six months?	Yes
1.2	Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment as follows:  <b>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</b>	
1.2.1a	Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?	Yes

1.2.1b	Is all other inbound and outbound traffic specifically denied (for example by using an explicit “deny all” or an implicit deny after allow statement)?	Yes
1.2.2	Are router configuration files secured from unauthorized access and synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted)?	Yes
1.2.3	Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?	Yes
1.3	Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:	
1.3.1	Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?	Yes
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	Yes
1.3.3	Are direct connections prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?	Yes
1.3.4	Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network?  (For example, block traffic originating from the internet with an internal address.)	Yes
1.3.5	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	Yes
1.3.6	Is stateful inspection, also known as dynamic packet filtering, implemented—that is, only established connections are allowed into the network?	Yes
1.3.7	Are system components that store cardholder data (such as a database) placed in an internal network zone, segregated from the DMZ and other untrusted networks?	Yes
1.3.8a	Are methods in place to prevent the disclosure of private IP addresses and routing information to the Internet?  <b>Note:</b> <i>Methods to obscure IP addressing may include, but are not limited to:</i> <ul style="list-style-type: none"> <li>· Network Address Translation (NAT)</li> <li>· Placing servers containing cardholder data behind proxy servers/firewalls,</li> <li>· Removal or filtering of route advertisements for private networks that employ registered addressing,</li> <li>· Internal use of RFC1918 address space instead of registered addresses.</li> </ul>	Yes
1.3.8b	Is any disclosure of private IP addresses and routing information to external entities authorized?	Yes
1.4a	Is personal firewall software installed and active on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network?	Yes
1.4b	Is the personal firewall software configured to specific configuration settings, actively running, and not alterable by users of mobile and/or employee-owned devices?	Yes

---

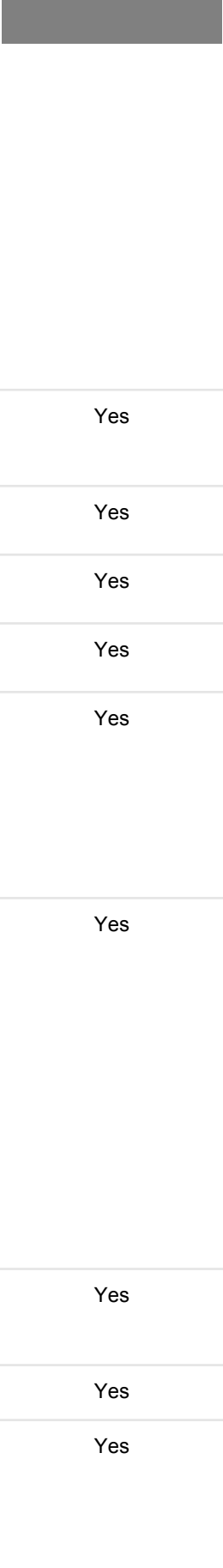
1.5	Are security policies and operational procedures for managing firewalls: <ul style="list-style-type: none"><li>· Documented</li><li>· In use</li><li>· Known to all affected parties?</li></ul>	Yes
-----	---	-----

---

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

	PCI DSS Question	Response:
2.1a	<p>Are vendor-supplied defaults always changed before installing a system on the network?</p> <p><i>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).</i></p>	Yes
2.1b	Are unnecessary default accounts removed or disabled before installing a system on the network?	Yes
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:	
2.1.1a	Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?	Yes
2.1.1b	Are default SNMP community strings on wireless devices changed at installation?	Yes
2.1.1c	Are default passwords/passphrases on access points changed at installation?	Yes
2.1.1d	Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	Yes
2.1.1e	Are other security-related wireless vendor defaults changed, if applicable?	Yes
2.2a	<p>Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards?</p> <p><i>Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).</i></p>	Yes
2.2b	Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?	Yes
2.2c	Are system configuration standards applied when new systems are configured?	Yes
2.2d	<p>Do system configuration standards include the following:</p> <ul style="list-style-type: none"> <li>· Changing of all vendor-supplied defaults and elimination of unnecessary default accounts?</li> <li>· Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server?</li> <li>· Enabling only necessary services, protocols, daemons, etc., as required for the function of the system?</li> <li>· Implementing additional security features for any required services, protocols or daemons that are considered to be insecure?</li> <li>· Configuring system security parameters to prevent misuse?</li> <li>· Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers?</li> </ul>	Yes

2.2.1a	<p>Is only one primary function implemented per server, to prevent functions that require different security levels from co-existing on the same server?</p> <p><i>For example, web servers, database servers, and DNS should be implemented on separate servers.</i></p>	Yes
2.2.1b	<p>If virtualization technologies are used, is only one primary function implemented per virtual system component or device?</p>	Yes
2.2.2a	<p>Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?</p>	Yes
2.2.2b	<p>Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?</p>	Yes
2.2.3	<p>Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure?</p> <p><i>For example, use secured technologies such as SSH, S-FTP, SSL or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.</i></p> <p><b>Note:</b> SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.</p>	Yes
2.2.4a	<p>Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?</p>	Yes
2.2.4b	<p>Are common system security parameters settings included in the system configuration standards?</p>	Yes
2.2.4c	<p>Are security parameter settings set appropriately on system components?</p>	Yes
2.2.5a	<p>Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?</p>	Yes
2.2.5b	<p>Are enabled functions documented and do they support secure configuration?</p>	Yes
2.2.5c	<p>Is only documented functionality present on system components?</p>	Yes

2.3	<p>Is non-console administrative access encrypted as follows:</p> <p><i>Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</i></p> <p><b>Note:</b> SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS.</p> <p>POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.</p>	
2.3a	<p>Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?</p>	
2.3b	<p>Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?</p>	Yes
2.3c	<p>Is administrator access to web-based management interfaces encrypted with strong cryptography?</p>	Yes
2.3d	<p>For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?</p>	Yes
2.3e	<p>For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:</p> <p>Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?</p>	Yes
2.3f	<p>For all other environments using SSL and/or early TLS:</p> <p>Does the documented Risk Mitigation and Migration Plan include the following?</p> <ul style="list-style-type: none"> <li>·Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;</li> <li>·Risk assessment results and risk reduction controls in place;</li> <li>·Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;</li> <li>·Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;</li> <li>·Overview of migration project plan including target migration completion date no later than 30th June 2016.</li> </ul>	Yes
2.4a	<p>Is an inventory maintained for systems components that are in scope for PCI DSS, including a list of hardware and software components and a description of function/use for each?</p>	Yes
2.4b	<p>Is the documented inventory kept current?</p>	Yes
2.5	<p>Are security policies and operational procedures for managing vendor defaults and other security parameters:</p> <ul style="list-style-type: none"> <li>·Documented</li> <li>·In use</li> <li>·Known to all affected parties?</li> </ul>	Yes



2.6

If you are a shared hosting provider, are your systems configured to protect each entity's (your customers') hosted environment and cardholder data?

Yes

*See Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for specific requirements that must be met.*

## Protect Cardholder Data

### Requirement 3: Protect stored cardholder data

	PCI DSS Question	Response:
3.1	Are data-retention and disposal policies, procedures, and processes implemented as follows:	
3.1a	Is data storage amount and retention time limited to that required for legal, regulatory, and business requirements?	Yes
3.1b	Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, or business reasons?	Yes
3.1c	Are there specific retention requirements for cardholder data?  <i>For example, cardholder data needs to be held for X period for Y business reasons.</i>	Yes
3.1d	Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?	Yes
3.1e	Does all stored cardholder data meet the requirements defined in the data-retention policy?	Yes
3.2a	For issuers and/or companies that support issuing services and store sensitive authentication data, is there a documented business justification for the storage of sensitive authentication data?	Yes
3.2b	For issuers and/or companies that support issuing services and store sensitive authentication data: Is the data secured?	Yes
3.2c	Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	Yes
3.2d	Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):	
3.2.1	The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization?  <i>This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</i>  <i>Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i> <ul style="list-style-type: none"> <li>·The cardholder's name,</li> <li>·Primary account number (PAN),</li> <li>·Expiration date, and</li> <li>·Service code</li> </ul> <i>To minimize risk, store only these data elements as needed for business.</i>	Yes
3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?	Yes
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	Yes

3.3	<p>Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see the full PAN?</p> <p><b>Note:</b> <i>This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.</i></p>	Yes
3.4	<p>Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using any of the following approaches?</p> <ul style="list-style-type: none"> <li>· One-way hashes based on strong cryptography (hash must be of the entire PAN)</li> <li>· Truncation (hashing cannot be used to replace the truncated segment of PAN)</li> <li>· Index tokens and pads (pads must be securely stored)</li> <li>· Strong cryptography with associated key management processes and procedures.</li> </ul> <p><b>Note:</b> <i>It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.</i></p>	Yes
3.4.1	<p>If disk encryption (rather than file- or column-level database encryption) is used, is access managed as follows:</p>	
3.4.1a	<p>Is logical access to encrypted file systems managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials)?</p>	Yes
3.4.1b	<p>Are cryptographic keys stored securely (for example, stored on removable media that is adequately protected with strong access controls)?</p>	Yes
3.4.1c	<p>Is cardholder data on removable media encrypted wherever stored?</p> <p><b>Note:</b> <i>This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be at least as strong as the data-encrypting key.</i></p>	Yes
3.5	<p>Are keys used to secure stored cardholder data protected against disclosure and misuse as follows:</p> <p><b>Note:</b> <i>This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be at least as strong as the data-encrypting key.</i></p>	
3.5.1	<p>Is access to cryptographic keys restricted to the fewest number of custodians necessary?</p>	Yes

3.5.2	<p>Are secret and private cryptographic keys used to encrypt/decrypt cardholder data stored in in one (or more) of the following forms at all times?</p> <ul style="list-style-type: none"> <li>· Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key</li> <li>· Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device)</li> <li>· As at least two full-length key components or key shares, in accordance with an industry-accepted method.</li> </ul> <p><b>Note: It is not required that public keys be stored in one of these forms.</b></p>	Yes
3.5.3	Are cryptographic keys stored in the fewest possible locations?	Yes
3.6a	Are all key-management processes and procedures fully documented and implemented for cryptographic keys used for encryption of cardholder data?	Yes
3.6b	<i>For service providers only:</i> If keys are shared with customers for transmission or storage of cardholder data, is documentation provided to customers that includes guidance on how to securely transmit, store and update customer's keys, in accordance with requirements 3.6.1 through 3.6.8 below?	Yes
3.6c	Are key-management processes and procedures implemented to require the following:	
3.6.1	Do cryptographic key procedures include the generation of strong cryptographic keys?	Yes
3.6.2	Do cryptographic key procedures include secure cryptographic key distribution?	Yes
3.6.3	Do cryptographic key procedures include secure cryptographic key storage?	Yes
3.6.4	Do cryptographic key procedures include cryptographic key changes for keys that have reached the end of their defined cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57)?	Yes
3.6.5a	Do cryptographic key procedures include retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key)?	Yes
3.6.5b	Do cryptographic key procedures include replacement of known or suspected compromised keys?	Yes
3.6.5c	If retired or replaced cryptographic keys are retained, are these keys only used for decryption/verification purposes, and not used for encryption operations?	Yes

<p>3.6.6</p>	<p>If manual clear-text key-management operations are used, do cryptographic key procedures include split knowledge and dual control of cryptographic keys as follows:</p> <ul style="list-style-type: none"> <li>·Do split knowledge procedures require that key components are under the control of at least two people who only have knowledge of their own key components?</li> </ul> <p>AND</p> <ul style="list-style-type: none"> <li>·Do dual control procedures require that at least two people are required to perform any key management operations and no one person has access to the authentication materials (for example, passwords or keys) of another?</li> </ul> <p><b>Note:</b> <i>Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.</i></p>	<p>Yes</p>
<p>3.6.7</p>	<p>Do cryptographic key procedures include the prevention of unauthorized substitution of cryptographic keys?</p>	<p>Yes</p>
<p>3.6.8</p>	<p>Are cryptographic key custodians required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities?</p>	<p>Yes</p>
<p>3.7</p>	<p>Are security policies and operational procedures for protecting stored cardholder data:</p> <ul style="list-style-type: none"> <li>·Documented</li> <li>·In use</li> <li>·Known to all affected parties?</li> </ul>	<p>Yes</p>

## Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Question	Response:	
<p>4.1a Are strong cryptography and security protocols, such as SSL/TLS, SSH or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?</p> <p><i>Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).</i></p> <p><b>Note:</b> SSL and early TLS are not considered strong cryptography and cannot be used as a security control after 30th June, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after 30th June, 2016.</p>	Yes	
4.1b	Are only trusted keys and/or certificates accepted?	Yes
4.1c	Are security protocols implemented to use only secure configurations, and to not support insecure versions or configurations?	Yes
4.1d	Is the proper encryption strength implemented for the encryption methodology in use (check vendor recommendations/best practices)?	Yes
4.1e	<p>For TLS implementations, is TLS enabled whenever cardholder data is transmitted or received?</p> <p><i>For example, for browser-based implementations: "HTTPS" appears as the browser Universal Record Locator (URL) protocol, and</i></p> <p><i>·Cardholder data is only requested if "HTTPS" appears as part of the URL.</i></p>	Yes
4.1f	<p>For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:</p> <p>Is there documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS?</p>	Yes

4.1g	<p>For all other environments using SSL and/or early TLS: Does the documented Risk Mitigation and Migration Plan include the following?</p> <ul style="list-style-type: none"> <li>·Description of usage, including; what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;</li> <li>·Risk assessment results and risk reduction controls in place;</li> <li>·Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;</li> <li>·Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;</li> <li>·Overview of migration project plan including target migration completion date no later than 30th June 2016.</li> </ul>	Yes
4.1.1	<p>Are industry best practices (for example, IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment?</p> <p><i>Note: The use of WEP as a security control was prohibited.</i></p>	Yes
4.2a	<p>Are PANs rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, or chat)?</p>	Yes
4.2b	<p>Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?</p>	Yes
4.3	<p>Are security policies and operational procedures for encrypting transmissions of cardholder data:</p> <ul style="list-style-type: none"> <li>·Documented</li> <li>·In use</li> <li>·Known to all affected parties?</li> </ul>	Yes

## Maintain a Vulnerability Management Program

### Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

	PCI DSS Question	Response:
5.1	Is anti-virus software deployed on all systems commonly affected by malicious software?	Yes
5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?	Yes
5.1.2	Are periodic evaluations performed to identify and evaluate evolving malware threats in order to confirm whether those systems considered to not be commonly affected by malicious software continue as such?	Yes
5.2	Are all anti-virus mechanisms maintained as follows:	
5.2a	Are all anti-virus software and definitions kept current?	Yes
5.2b	Are automatic updates and periodic scans enabled and being performed?	Yes
5.2c	Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?	Yes
5.3	Are all anti-virus mechanisms: <ul style="list-style-type: none"> <li>·Actively running?</li> <li>·Unable to be disabled or altered by users?</li> </ul> <b>Note:</b> <i>Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.</i>	Yes
5.4	Are security policies and operational procedures for protecting systems against malware: <ul style="list-style-type: none"> <li>·Documented</li> <li>·In use</li> <li>·Known to all affected parties?</li> </ul>	Yes



## Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question	Response:
<p>6.1 Is there a process to identify security vulnerabilities, including the following:</p> <ul style="list-style-type: none"> <li>·Using reputable outside sources for vulnerability information?</li> <li>·Assigning a risk ranking to vulnerabilities that includes identification of all “high” risk and “critical” vulnerabilities?</li> </ul> <p><b>Note:</b> Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score and/or the classification by the vendor, and/or type of systems affected.</p> <p><i>Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process or transmit cardholder data.</i></p>	Yes
6.2a	Yes
6.2b	Yes
<p>6.2b Are critical security patches installed within one month of release?</p> <p><b>Note:</b> Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</p>	Yes
6.3a	Yes
6.3b	Yes
6.3c	Yes
6.3d	
6.3.1	Yes

6.3.2	<p>Is all custom code reviewed prior to release to production or customers to identify any potential coding vulnerability (using either manual or automated processes as follows:</p> <ul style="list-style-type: none"> <li>·Are code changes reviewed by individuals other than the originating code author, and by individuals who are knowledgeable about code review techniques and secure coding practices?</li> <li>·Do code reviews ensure code is developed according to secure coding guidelines?</li> <li>·Are appropriate corrections are implemented prior to release?</li> <li>·Are code review results are reviewed and approved by management prior to release?</li> </ul> <p><b>Note:</b> This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.</p>	Yes
6.4	Are change control processes and procedures followed for all changes to system components to include the following:	
6.4.1a	Are development/test environments separate from the production environment?	Yes
6.4.1b	Is access control in place to enforce the separation between the development/test environments and the production environment?	Yes
6.4.2	Is there separation of duties between personnel assigned to the development/test environments and those assigned to the production environment?	Yes
6.4.3	Are production data (live PANs) not used for testing or development?	Yes
6.4.4	Are test data and accounts removed before production systems become active?	Yes
6.4.5a	<p>Are change-control procedures for implementing security patches and software modifications documented and require the following?</p> <ul style="list-style-type: none"> <li>·Documentation of impact</li> <li>·Documented change control approval by authorized parties</li> <li>·Functionality testing to verify that the change does not adversely impact the security of the system</li> <li>·Back-out procedures</li> </ul>	Yes
6.4.5b	Are the following performed and documented for all changes:	
6.4.5.1	Documentation of impact?	Yes
6.4.5.2	Documented approval by authorized parties?	Yes
6.4.5.3a	Functionality testing to verify that the change does not adversely impact the security of the system?	Yes
6.4.5.3b	For custom code changes, testing of updates for compliance with PCI DSS Requirement 6.5 before being deployed into production?	Yes
6.4.5.4	Back-out procedures?	Yes
6.5a	Do software-development processes address common coding vulnerabilities?	Yes
6.5b	Are developers trained in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory?	Yes

6.5c	<p>Are applications developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities:</p> <p><b>Note:</b> <i>The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the Open Web Application Security Project (OWASP) Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.</i></p>	
6.5.1	<p>Do coding techniques address injection flaws, particularly SQL injection?</p> <p><b>Note:</b> <i>Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.</i></p>	Yes
6.5.2	Do coding techniques address buffer overflow vulnerabilities?	Yes
6.5.3	Do coding techniques address insecure cryptographic storage?	Yes
6.5.4	Do coding techniques address insecure communications?	Yes
6.5.5	Do coding techniques address improper error handling?	Yes
6.5.6	Do coding techniques address all “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)?	Yes
6.5.7a	For web applications and application interfaces (internal or external), are applications developed based on secure coding guidelines to protect applications from the following additional vulnerabilities:	
6.5.7b	Do coding techniques address cross-site scripting (XSS) vulnerabilities?	Yes
6.5.8	Do coding techniques address improper access control such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions?	Yes
6.5.9	Do coding techniques address cross-site request forgery (CSRF)?	Yes
6.5.10	<p>Do coding techniques address broken authentication and session management?</p> <p><b>Note:</b> <i>Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.</i></p>	Yes

<p>6.6</p>	<p>For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying either of the following methods?</p> <ul style="list-style-type: none"> <li>· Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows:                     <ul style="list-style-type: none"> <li>- At least annually</li> <li>- After any changes</li> <li>- By an organization that specializes in application security</li> <li>- That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment</li> <li>- That all vulnerabilities are corrected</li> <li>- That the application is re-evaluated after the corrections</li> </ul> </li> </ul> <p><b>Note:</b> This assessment is not the same as the vulnerability scans performed for Requirement 11.2.</p> <p><b>- OR -</b></p> <ul style="list-style-type: none"> <li>· Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) as follows:                     <ul style="list-style-type: none"> <li>- Is situated in front of public-facing web applications to detect and prevent web-based attacks.</li> <li>- Is actively running and up to date as applicable</li> <li>- Is generating audit logs</li> <li>- Is configured to either block web-based attacks, or generate an alert that is immediately investigated.</li> </ul> </li> </ul>	<p>Yes</p>
<p>6.7</p>	<p>Are security policies and operational procedures for developing and maintaining secure systems and applications:</p> <ul style="list-style-type: none"> <li>· Documented</li> <li>· In use</li> <li>· Known to all affected parties?</li> </ul>	<p>Yes</p>

## Implement Strong Access Control Measures

### Requirement 7: Restrict access to cardholder data by business need to know

	PCI DSS Question	Response:
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:	
7.1a	<ul style="list-style-type: none"> <li>· Is there a written policy for access control that incorporates the following?               <ul style="list-style-type: none"> <li>· Defining access needs and privilege assignments for each role</li> <li>· Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities,</li> <li>· Assignment of access based on individual personnel's job classification and function</li> <li>· Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved</li> </ul> </li> </ul>	Yes
7.1.1	Are access needs for each role defined, including: <ul style="list-style-type: none"> <li>· System components and data resources that each role needs to access for their job function?</li> <li>· Level of privilege required (for example, user, administrator, etc.) for accessing resources?</li> </ul>	Yes
7.1.2	Is access to privileged user IDs restricted as follows: <ul style="list-style-type: none"> <li>· To least privileges necessary to perform job responsibilities?</li> <li>· Assigned only to roles that specifically require that privileged access?</li> </ul>	Yes
7.1.3	Are access assigned based on individual personnel's job classification and function?	Yes
7.1.4	Is documented approval by authorized parties required, specifying required privileges?	Yes
7.2	Is an access control system in place for system components to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed, as follows:	
7.2.1	Are access control systems in place on all system components?	Yes
7.2.2	Are access control systems configured to enforce privileges assigned to individuals based on job classification and function?	Yes
7.2.3	Do access control systems have a default "deny-all" setting?	Yes
7.3	Are security policies and operational procedures for restricting access to cardholder data: <ul style="list-style-type: none"> <li>· Documented</li> <li>· In use</li> <li>· Known to all affected parties?</li> </ul>	Yes

## Requirement 8: Identify and authenticate access to system components

PCI DSS Question	Response:
8.1	[Redacted]
8.1.1	Yes
8.1.2	Yes
8.1.3	Yes
8.1.4	Yes
8.1.5a	Yes
8.1.5b	Yes
8.1.6a	Yes
8.1.6b	Yes
8.1.7	Yes
8.1.8	Yes
8.2	Yes
8.2.1a	Yes
8.2.1b	Yes
8.2.2	Yes
8.2.3a	Yes

8.2.3b	<p><i>For service providers only: Are non-consumer customer passwords required to meet the following minimum length and complexity requirements?</i></p> <ul style="list-style-type: none"> <li>· A minimum password length of at least seven characters</li> <li>· Contain both numeric and alphabetic characters</li> </ul>	Yes
8.2.4a	Are user passwords/passphrases changed at least every 90 days?	Yes
8.2.4b	<p><i>For service providers only: Are non-consumer customer passwords required to be changed periodically, and are non-consumer customers given guidance as to when, and under what circumstances, passwords must change.</i></p>	Yes
8.2.5a	Must an individual submit a new password/phrase that is different from any of the last four passwords/phrases he or she has used?	Yes
8.2.5b	<p><i>For service providers only: Are new, non-consumer customer passwords required to be different from any of the last four passwords used?</i></p>	Yes
8.2.6	Are passwords/phrases set to a unique value for each user for first-time use and upon reset, and must each user change their password immediately after the first use?	Yes
8.3	<p>Is two-factor authentication incorporated for remote network access originating from outside the network by personnel (including users and administrators) and all third parties (including vendor access for support or maintenance)?</p> <p><b>Note:</b> <i>Two-factor authentication requires that two of the three authentication methods (see PCI DSS Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.</i></p> <p><i>Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.</i></p>	Yes
8.4a	Are authentication procedures and policies documented and communicated to all users?	Yes
8.4b	<p>Do authentication procedures and policies include the following?</p> <ul style="list-style-type: none"> <li>· Guidance on selecting strong authentication credentials</li> <li>· Guidance for how users should protect their authentication credentials</li> <li>· Instructions not to reuse previously used passwords</li> <li>· Instructions that users should change passwords if there is any suspicion the password could be compromised</li> </ul>	Yes
8.5	<p>Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows:</p> <ul style="list-style-type: none"> <li>· Generic user IDs and accounts are disabled or removed;</li> <li>· Shared user IDs for system administration activities and other critical functions do not exist; and</li> <li>· Shared and generic user IDs are not used to administer any system components?</li> </ul>	Yes

8.5.1	<p>For service providers only: Do service providers with remote access to customer premises (for example, for support of POS systems or servers) use a unique authentication credential (such as a password/phrase) for each customer?</p> <p><b>Note:</b> This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.</p> <p><b>Note:</b> Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement.</p>	Yes
8.6	<p>Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, and certificates, etc.), is the use of these mechanisms assigned as follows?</p> <ul style="list-style-type: none"> <li>· Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts</li> <li>· Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access</li> </ul>	Yes
8.7	<p>Is all access to any database containing cardholder data (including access by applications, administrators, and all other users) restricted as follows:</p>	
8.7a	<p>Is all user access to, user queries of, and user actions on (for example, move, copy, delete), the database through programmatic methods only (for example, through stored procedures)?</p>	Yes
8.7b	<p>Is user direct access to or queries to of databases restricted to database administrators?</p>	Yes
8.7c	<p>Are application IDs only able to be used by the applications (and not by individual users or other processes)?</p>	Yes
8.8	<p>Are security policies and operational procedures for identification and authentication:</p> <ul style="list-style-type: none"> <li>· Documented</li> <li>· In use</li> <li>· Known to all affected parties?</li> </ul>	Yes



## Requirement 9: Restrict physical access to cardholder data

PCI DSS Question	Response:
9.1 Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	Yes
9.1.1a Are video cameras and/or access-control mechanisms in place to monitor individual physical access to sensitive areas? <i>Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder data. This excludes public-facing areas where only point-of-sale terminals are present such as the cashier areas in a retail store.</i>	Yes
9.1.1b Are video cameras and/or access-control mechanisms protected from tampering or disabling?	Yes
9.1.1c Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries?	Yes
9.1.1d Is data collected from video cameras and/or access control mechanisms stored for at least three months unless otherwise restricted by law?	Yes
9.1.2 Are physical and/or logical controls in place to restrict access to publicly accessible network jacks?  <i>For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.</i>	Yes
9.1.3 Is physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines restricted?	Yes
9.2a Are procedures developed to easily distinguish between onsite personnel and visitors, which include: · Identifying new onsite personnel or visitors (for example, assigning badges), · Changing access requirements, and · Revoking terminated onsite personnel and expired visitor identification (such as ID badges) <i>For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i>	Yes
9.2b Do identification methods (such as ID badges) clearly identify visitors and easily distinguish between onsite personnel and visitors?	Yes
9.2c Is access to the badge system limited to authorized personnel?	Yes
9.3 Is physical access to sensitive areas controlled for onsite personnel, as follows: · Is access authorized and based on individual job function? · Is access revoked immediately upon termination · Upon termination, are all physical access mechanisms, such as keys, access cards, etc., returned or disabled?	Yes
9.4 Is visitor identification and access handled as follows:	

9.4.1	Are visitors authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained?	Yes
9.4.2a	Are visitors identified and given a badge or other identification that visibly distinguishes the visitors from onsite personnel?	Yes
9.4.2b	Do visitor badges or other identification expire?	Yes
9.4.3	Are visitors asked to surrender the badge or other identification before leaving the facility or at the date of expiration?	Yes
9.4.4a	Is a visitor log in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted?	Yes
9.4.4b	Does the visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access?	Yes
9.4.4c	Is the visitor log retained for at least three months?	Yes
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?  <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i>	Yes
9.5.1a	Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?	Yes
9.5.1b	Is this location's security reviewed at least annually?	Yes
9.6a	Is strict control maintained over the internal or external distribution of any kind of media?	Yes
9.6b	Do controls include the following:	
9.6.1	Is media classified so the sensitivity of the data can be determined?	Yes
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	Yes
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	Yes
9.7	Is strict control maintained over the storage and accessibility of media?	Yes
9.7.1a	Are inventory logs of all media properly maintained?	Yes
9.7.1b	Are periodic media inventories conducted at least annually?	Yes
9.8a	Is all media destroyed when it is no longer needed for business or legal reasons?	Yes
9.8b	Is there a periodic media destruction policy that defines requirements for the following? <ul style="list-style-type: none"> <li>·Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.</li> <li>·Storage containers used for materials that are to be destroyed must be secured.</li> <li>·Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program (in accordance with industry-accepted standards for secure deletion), or by physically destroying the media.</li> </ul>	Yes

9.8c	Is media destruction performed as follows:	
9.8.1a	Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	Yes
9.8.1b	Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	Yes
9.8.2	Is cardholder data on electronic media rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media, so that cardholder data cannot be reconstructed?	Yes
9.9	<p>Are devices that capture payment card data via direct physical interaction with the card protected against tampering and substitution as follows?</p> <p><b>Note:</b> This requirement applies to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.</p> <p><b>Note:</b> Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.</p>	
9.9a	Do policies and procedures require that a list of such devices maintained?	Yes
9.9b	Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	Yes
9.9c	Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	Yes
9.9.1a	<p>Does the list of devices include the following?</p> <ul style="list-style-type: none"> <li>· Make, model of device</li> <li>· Location of device (for example, the address of the site or facility where the device is located)</li> <li>· Device serial number or other method of unique identification</li> </ul>	Yes
9.9.1b	Is the list accurate and up to date?	Yes
9.9.1c	Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	Yes
9.9.2a	<p>Are device surfaces periodically inspected to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows?</p> <p><b>Note:</b> Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.</p>	Yes
9.9.2b	Are personnel are aware of procedures for inspecting devices?	Yes
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?	

9.9.3a	<p>Do training materials for personnel at point-of-sale locations include the following?</p> <ul style="list-style-type: none"> <li>·Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.</li> <li>·Do not install, replace, or return devices without verification.</li> <li>·Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).</li> <li>·Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).</li> </ul>	Yes
9.9.3b	<p>Have personnel at point-of-sale locations received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices?</p>	Yes
9.10	<p>Are security policies and operational procedures for restricting physical access to cardholder data:</p> <ul style="list-style-type: none"> <li>·Documented</li> <li>·In use</li> <li>·Known to all affected parties?</li> </ul>	Yes

## Regularly Monitor and Test Networks

### Requirement 10: Track and monitor all access to network resources and cardholder data

	PCI DSS Question	Response:
10.1a	Are audit trails enabled and active for system components?	Yes
10.1b	Is access to system components linked to individual users?	Yes
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:	
10.2.1	All individual user accesses to cardholder data?	Yes
10.2.2	All actions taken by any individual with root or administrative privileges?	Yes
10.2.3	Access to all audit trails?	Yes
10.2.4	Invalid logical access attempts?	Yes
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges?	Yes
10.2.6	Initialization, stopping, or pausing of the audit logs?	Yes
10.2.7	Creation and deletion of system-level object?	Yes
10.3	Are the following audit trail entries recorded for all system components for each event:	
10.3.1	User identification?	Yes
10.3.2	Type of event?	Yes
10.3.3	Date and time?	Yes
10.3.4	Success or failure indication?	Yes
10.3.5	Origination of event?	Yes
10.3.6	Identity or name of affected data, system component, or resource?	Yes
10.4	Are all critical system clocks and times synchronized through use of time synchronization technology, and is the technology kept current?	Yes
	<b>Note:</b> One example of time synchronization technology is Network Time Protocol (NTP).	
10.4.1	Are the following processes implemented for critical systems to have the correct and consistent time:	
10.4.1a	Do only designated central time server(s) receive time signals from external sources, and are time signals from external sources based on International Atomic Time or UTC?	Yes
10.4.1b	Where there is more than one designated time server, do the time servers peer with each other to keep accurate time?	Yes
10.4.1c	Do systems receive time only from designated central time server(s)?	Yes

10.4.2a	Is time data is protected as follows:  Is access to time data restricted to only personnel with a business need to access time data?	Yes
10.4.2b	Are changes to time settings on critical systems logged, monitored, and reviewed?	Yes
10.4.3	Are time settings received from specific, industry-accepted time sources? (This is to prevent a malicious individual from changing the clock).  <i>Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).</i>	Yes
10.5	Are audit trails secured so they cannot be altered, as follows:	
10.5.1	Is viewing of audit trails limited to those with a job-related need?	Yes
10.5.2	Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?	Yes
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	Yes
10.5.4	Are logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) written onto a secure, centralized, internal log server or media?	Yes
10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	Yes
10.6	Are logs and security events for all system components reviewed to identify anomalies or suspicious activity as follows?  <b>Note:</b> <i>Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.</i>	
10.6.1a	Are written policies and procedures defined for reviewing the following at least daily, either manually or via log tools? ·All security events ·Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD ·Logs of all critical system components ·Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	Yes
10.6.1b	Are the above logs and security events reviewed at least daily?	Yes
10.6.2a	Are written policies and procedures defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization’s policies and risk management strategy?	Yes
10.6.2b	Are reviews of all other system components performed in accordance with organization’s policies and risk management strategy?	Yes
10.6.3a	Are written policies and procedures defined for following up on exceptions and anomalies identified during the review process?	Yes

10.6.3b	Is follow up to exceptions and anomalies performed?	Yes
10.7a	Are audit log retention policies and procedures in place and do they require that logs are retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)?	Yes
10.7b	Are audit logs retained for at least one year?	Yes
10.7c	Are at least the last three months' logs immediately available for analysis?	Yes
10.8	Are security policies and operational procedures for monitoring all access to network resources and cardholder data: <ul style="list-style-type: none"> <li>· Documented</li> <li>· In use</li> <li>· Known to all affected parties?</li> </ul>	Yes

## Requirement 11: Regularly test security systems and processes

PCI DSS Question	Response:
<p>11.1a Are processes implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis?</p> <p><i><b>Note:</b> Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.</i></p> <p><i>Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.</i></p>	Yes
<p>11.1b Does the methodology detect and identify any unauthorized wireless access points, including at least the following?</p> <ul style="list-style-type: none"> <li>·WLAN cards inserted into system components;</li> <li>·Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and</li> <li>·Wireless devices attached to a network port or network device.</li> </ul>	Yes
<p>11.1c If wireless scanning is utilized to identify authorized and unauthorized wireless access points, is the scan performed at least quarterly for all system components and facilities?</p>	Yes
<p>11.1d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), is monitoring configured to generate alerts to notify personnel?</p>	Yes
<p>11.1.1 Is an inventory of authorized wireless access points maintained and a business justification documented for all authorized wireless access points?</p>	Yes
<p>11.1.2a Does the incident response plan define and require a response in the event that an unauthorized wireless access point is detected?</p>	Yes
<p>11.1.2b Is action taken when unauthorized wireless access points are found?</p>	Yes
<p>11.2 Are internal and external network vulnerability scans run at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), as follows?</p> <p><i><b>Note:</b> Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.</i></p> <p><i>For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.</i></p>	
<p>11.2.1a Are quarterly internal vulnerability scans performed?</p>	Yes



11.2.1b	Does the quarterly internal scan process include rescans as needed until all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	Yes
11.2.1c	Are quarterly internal scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	Yes
11.2.2a	Are quarterly external vulnerability scans performed?  <b>Note:</b> Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).  <i>Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.</i>	Yes
11.2.2b	Do external quarterly scan and rescan results satisfy the ASV Program Guide requirements for a passing scan (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures)?	Yes
11.2.2c	Are quarterly external vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV)?	Yes
11.2.3a	Are internal and external scans, and rescans as needed, performed after any significant change?  <b>Note:</b> Scans must be performed by qualified personnel.	Yes
11.2.3b	Does the scan process include rescans until: ·For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS, ·For internal scans, a passing result is obtained or all “high-risk” vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved?	Yes
11.2.3c	Are scans performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	Yes
11.3	Does the penetration-testing methodology include the following? ·Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) ·Includes coverage for the entire CDE perimeter and critical systems ·Includes testing from both inside and outside the network ·Includes testing to validate any segmentation and scope-reduction controls ·Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 ·Defines network-layer penetration tests to include components that support network functions as well as operating systems ·Includes review and consideration of threats and vulnerabilities experienced in the last 12 months ·Specifies retention of penetration testing results and remediation activities results	Yes
11.3.1a	Is <i>external</i> penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	Yes
11.3.1b	Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	Yes

11.3.2a	Is <i>internal</i> penetration testing performed per the defined methodology, at least annually, and after any significant infrastructure or application changes to the environment (such as an operating system upgrade, a sub-network added to the environment, or an added web server)?	Yes
11.3.2b	Are tests performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV)?	Yes
11.3.3	Are exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections?	Yes
11.3.4	If segmentation is used to isolate the CDE from other networks:	
11.3.4a	Are penetration-testing procedures defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems in the CDE?	Yes
11.3.4b	Does penetration testing to verify segmentation controls meet the following? <ul style="list-style-type: none"> <li>·Performed at least annually and after any changes to segmentation controls/methods</li> <li>·Covers all segmentation controls/methods in use</li> <li>·Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems in the CDE.</li> </ul>	Yes
11.4a	Are intrusion-detection and/or intrusion-prevention techniques that detect and/or prevent intrusions into the network in place to monitor all traffic: <ul style="list-style-type: none"> <li>·At the perimeter of the cardholder data environment, and</li> <li>·At critical points in the cardholder data environment</li> </ul>	Yes
11.4b	Are intrusion-detection and/or intrusion-prevention techniques configured to alert personnel of suspected compromises?	Yes
11.4c	Are all intrusion-detection and prevention engines, baselines, and signatures kept up-to-date?	Yes
11.5a	Is a change-detection mechanism (for example, file-integrity monitoring tools) deployed within the cardholder data environment to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files? <p><i>Examples of files that should be monitored include:</i></p> <ul style="list-style-type: none"> <li>·System executables</li> <li>·Application executables</li> <li>·Configuration and parameter files</li> <li>·Centrally stored, historical or archived, log, and audit files</li> <li>·Additional critical files determined by entity (for example, through risk assessment or other means)</li> </ul>	Yes
11.5b	Is the change-detection mechanism configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files, and do the tools perform critical file comparisons at least weekly? <p><b>Note:</b> For change detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).</p>	Yes

11.5.1	Is a process in place to respond to any alerts generated by the change-detection solution?	Yes
11.6	Are security policies and operational procedures for security monitoring and testing: · Documented · In use · Known to all affected parties?	Yes

## Maintain an Information Security Policy

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

	PCI DSS Question	Response:
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?	Yes
12.1.1	Is the security policy reviewed at least annually and updated when the environment changes?	Yes
12.2a	Is an annual risk assessment process implemented that identifies assets, threats, and vulnerabilities? <ul style="list-style-type: none"> <li>·Identifies critical assets, threats, and vulnerabilities, and</li> <li>·Results in a formal, documented analysis of risk?</li> </ul> <p><i>Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.</i></p>	Yes
12.2b	Is the risk assessment process performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)?	Yes
12.3	Are usage policies for critical technologies developed to define proper use of these technologies and require the following:  <p><b>Note:</b> <i>Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.</i></p>	
12.3.1	Explicit approval by authorized parties to use the technologies?	Yes
12.3.2	Authentication for use of the technology?	Yes
12.3.3	A list of all such devices and personnel with access?	Yes
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)?	Yes
12.3.5	Acceptable uses of the technologies?	Yes
12.3.6	Acceptable network locations for the technologies?	Yes
12.3.7	List of company-approved products?	Yes
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	Yes
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use?	Yes
12.3.10a	For personnel accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need?  <p><i>Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.</i></p>	Yes

12.3.10b	For personnel with proper authorization, does the policy require the protection of cardholder data in accordance with PCI DSS Requirements?	Yes
12.4	Do the security policy and procedures clearly define information security responsibilities for all personnel?	Yes
12.5a	Is responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management?	Yes
12.5b	Are the following information security management responsibilities formally assigned to an individual or team:	
12.5.1	Establishing, documenting, and distributing security policies and procedures?	Yes
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?	Yes
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	Yes
12.5.4	Administering user accounts, including additions, deletions, and modifications?	Yes
12.5.5	Monitoring and controlling all access to data?	Yes
12.6a	Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?	Yes
12.6b	Do security awareness program procedures include the following:	
12.6.1a	Does the security awareness program provide multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions)?  <i>Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.</i>	Yes
12.6.1b	Are personnel educated upon hire and at least annually?	Yes
12.6.1c	Have employees completed awareness training and are they aware of the importance of cardholder data security?	Yes
12.6.2	Are personnel required to acknowledge at least annually that they have read and understood the company's security policy and procedures?	Yes
12.7	Are potential personnel (see definition of "personnel" above) screened prior to hire to minimize the risk of attacks from internal sources?  <i>Examples of background checks include previous employment history, criminal record, credit history and reference checks.</i>  <i>Note: For those potential personnel to be hired for certain positions, such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i>	Yes
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	
12.8.1	Is a list of service providers maintained?	Yes

12.8.2	<p>Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?</p> <p><i>Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</i></p>	Yes
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	Yes
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	Yes
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	Yes
12.9	<p><i>For service providers only:</i> Do service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment?</p> <p><i>Note: This requirement is a best practice until June 30, 2015, after which it becomes a requirement.</i></p> <p><i>Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</i></p>	Yes
12.10	Has an incident response plan been implemented in preparation to respond immediately to a system breach, as follows:	
12.10.1a	Has an incident response plan been created to be implemented in the event of system breach?	Yes
12.10.1b	Does the plan address the following, at a minimum:	
12.10.1.1	·Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum?	Yes
12.10.1.2	·Specific incident response procedures?	Yes
12.10.1.3	·Business recovery and continuity procedures?	Yes
12.10.1.4	·Data back-up processes?	Yes
12.10.1.5	·Analysis of legal requirements for reporting compromises?	Yes
12.10.1.6	·Coverage and responses of all critical system components?	Yes
12.10.1.7	·Reference or inclusion of incident response procedures from the payment brands?	Yes
12.10.2	Is the plan tested at least annually?	Yes

12.10.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?	Yes
12.10.4	Is appropriate training provided to staff with security breach response responsibilities?	Yes
12.10.5	Are alerts from security monitoring systems included in the incident response plan?	Yes
12.10.6	Is process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?	Yes