Service Provider PCI-DSS Responsibility Matrix

Pursuant to PCI-DSS requirements, Company (as defined in the Master Service Agreement, and identified as a "Service Provider" in PCI-DSS) is required to acknowledge in writing to its customers that Company may be responsible for the security of managing network components of Customer (as defined in the Master Service Agreement) Cardholder Data Environment ("CDE"), such as routers, firewalls, databases, physical security, or servers. Despite management of some network components of the Customer CDE, use of Company's services does not relieve the Customer of ultimate responsibility for its own PCI-DSS compliance, or exempt the Customer from any accountability and obligation it may have under PCI-DSS to ensure cardholder data and CDE are secure. The terms and conditions of the Master Service Agreement are incorporated into this Responsibility Matrix.

Note: Customized solutions may have a different responsibility matrix which is available on request.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS			
Requirement 1: Install and maintain a firewall configuration to protect cardholder data			
1.1	Establish and implement firewall and router configuration standards that include the following:		
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	Customer	Customer is responsible for its internet firewall.
1.1.2	(a) A current network diagram that documents all connections between the CDE and other networks, including any wireless networks	Shared	Company is responsible for its own environment, including network diagrams, system configuration security, justification for ports, protocols, services and daemons. Customer is responsible for all connections between the CDE and other networks.
	(b) A process to ensure the diagram is kept current		
1.1.3	(a) A current diagram that shows all cardholder data flows across systems and networks	Customer	Customer is responsible for all cardholder data flows across systems and networks and for keeping it current.
	(b) A process to ensure the diagram is kept current		
1.1.4	(a) Firewall is required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Customer	Customer is responsible for the environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) Is the current network diagram consistent with the firewall configuration standards	Customer	Customer is responsible for the environment.
1.1.6	(a) Firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each	Customer	Customer is responsible for the environment.
	(b) All insecure services, protocols, and ports are identified, and security features are documented and implemented for each identified service	Shared	Customer and Company are responsible for the own environments.
1.1.7	(a) Firewall and router configuration standards require review of firewall and router rule sets at least every six months	Customer	Customer is responsible for its environment.
	(b) Firewall and router rule sets are reviewed at least every six months	Customer	Customer is responsible for its environment.
1.2	Firewall and router configurations restrict connections between untrusted networks and any system in the CDE as follows: ***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.*	Customer	Customer is responsible for the CDE.
1.2.1	(a) Inbound and outbound traffic is restricted to that which is necessary for the CDE		
	(b) Inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)		
1.2.2	Router configuration files are secured from unauthorized access and synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted)	Customer	Customer is responsible for the CDE.
1.2.3	Perimeter firewalls are installed between all wireless networks and the CDE, 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 CDE	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
1.3	Direct public access is prohibited between the Internet and any system component in the CDE, as follows:	Customer	Customer is responsible for the CDE.
1.3.1	A DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports	Customer	Customer is responsible for the CDE.
1.3.2	Inbound Internet traffic is limited to IP addresses within the DMZ	Customer	Customer is responsible for the CDE.
1.3.3	Anti-spoofing measures are 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.)	Customer	Customer is responsible for the CDE.
1.3.4	Outbound traffic from the CDE to the Internet is explicitly authorized	Customer	Customer is responsible for the CDE.
1.3.5	Only established connections are permitted into the network	Customer	Customer is responsible for the CDE.
1.3.6	System components that store cardholder data (such as a database) are placed in an internal network zone, segregated from the DMZ and other untrusted networks	Customer	Customer is responsible for the CDE.
1.3.7	(a) Methods are in place to prevent the disclosure of private IP addresses and routing information to the Internet ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	Shared	Company is responsible for non-disclosure of private IP addressing and routing information. Customer is responsible for the CDE and any servers containing cardholder data.
	(b) Disclosure of private IP addresses and routing information to external entities has to be authorized.		

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
1.4	(a) Personal firewall software (or equivalent functionality) is installed and active on any portable computing devices (including Company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE	Customer	Customer is responsible for the CDE.
1.5	Are security policies and operational procedures for managing firewalls: • Documented • In use • Known to all affected parties		
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters			
2.1	(a) Vendor-supplied defaults are always changed before installing a system on the network ***Note:*** *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, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).*	Shared	Company has the responsibility to change vendor-supplied default passwords prior to network elements being installed; removing or disabling unnecessary default accounts before installing any network element; configuring all network elements consistent with industry-accepted hardening standards and common security parameters and fully documenting the configuration. Where possible and hardware allows, Company will use TLS and SNMP for strong cryptography between its network elements and systems. Customer is responsible for changing vendor-supplied default passwords prior to systems being installed; removing or disabling unnecessary default accounts before installing any network system, and; changing all wireless vendor defaults within the CDE.
	(b) Unnecessary default accounts are removed or disabled before installing a system on the network		
2.1.1	For wireless environments connected to the CDE or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:		
	(a) Encryption keys are changed from default at installation, and changed anytime anyone with knowledge of the keys leaves Company or changes positions		
	(b) Default SNMP community strings on wireless devices are changed at installation		
	(c) Default passwords/passphrases on access points are changed at installation		

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(d) Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks		
	(e) Other security-related wireless vendor defaults are changed, if applicable		
2.2	(a) Configuration standards are developed for all system components and are they consistent with industry-accepted system hardening standards. ***Note:*** *Sources of industry-accepted system hardening standards may include, but are not limited to, Sys Admin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).*	Shared	
	(b) System configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.	Shared	Customer and Company are responsible for the own environment.
	(c) System configuration standards are applied when new systems are configured	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(d) System configuration standards include all of the following: • Changing of all vendor-supplied defaults and elimination of unnecessary default accounts • Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server • Enabling only necessary services, protocols, daemons, etc., as required for the function of the system • Implementing additional security features for any required services, protocols or daemons that are considered to be insecure • Configuring system security parameters to prevent misuse • Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers	Shared	Customer and Company are responsible for the own environment.
2.2.1	(a) Only one primary function is implemented per server, to prevent functions that require different security levels from co-existing on the same server *For example, web servers, database servers, and DNS should be implemented on separate servers.*	Shared	Customer and Company are responsible for the own environment.
	(b) If virtualization technologies are used, only one primary function is implemented per virtual system component or device	Shared	Customer and Company are responsible for the own environment.
2.2.2	(a) Only necessary services, protocols, daemons, etc. are enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)	Shared	Customer and Company are responsible for the own environment.
	(b) All enabled insecure services, daemons, or protocols are justified per documented configuration standards	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
2.2.3	Additional security features are documented and implemented for any required services, protocols or daemons that are considered to be insecure ***Note:*** *SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2 of the PCI Data Security Standard.*	Shared	Customer and Company are responsible for the own environment.
2.2.4	(a) System administrators and/or personnel that configure system components are knowledgeable about common security parameter settings for those system components	Shared	Customer and Company are responsible for the own environment.
	(b) Common system security parameters settings are included in the system configuration standards	Shared	Customer and Company are responsible for the own environment.
	(c) Security parameter settings are set appropriately on system components	Shared	Customer and Company are responsible for the own environment.
2.2.5	(a) All unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers— have been removed	Shared	Customer and Company are responsible for the own environment.
	(b) Enabled functions are documented, and do they support secure configuration	Shared	Customer and Company are responsible for the own environment.
	(c) Only documented functionality is present on system components	Shared	Customer and Company are responsible for the own environment.
2.3	Non-console administrative access is encrypted as follows: ***Note:*** *SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2 of the PCI Data Security Standard.*	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	Non-console administrative access is encrypted as follows: ***Note*:** *SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2 of the PCI Data Security Standard.*	Shared	Customer and Company are responsible for the own environment.
	(a) All non-console administrative access is encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested	Shared	Customer and Company are responsible for the own environment.
	(b) System services and parameter files are configured to prevent the use of Telnet and other insecure remote login commands	Shared	Customer and Company are responsible for the own environment.
	(c) Administrator access to web-based management interfaces is encrypted with strong cryptography	Shared	Customer and Company are responsible for the own environment.
	(d) For the technology in use, strong cryptography is implemented according to industry best practice and/or vendor recommendations	Shared	Customer and Company are responsible for the own environment.
2.4	(a) An inventory is 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	Shared	Customer and Company are responsible for the own environment.
	(b) The documented inventory is kept current	Shared	Customer and Company are responsible for the own environment.
2.5	Are security policies and operational procedures for managing vendor defaults and other security parameters: • Documented • In use • Known to all affected parties	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
2.6	If you are a shared hosting provider, your systems are configured to protect each entity's (your Customers') hosted environment and cardholder data ***Note:*** *See Appendix A1 of the PCI Data Security Standard for specific requirements that must be met.*	N/A	N/A
PROTECT CARDHOLDER DATA			
Requirement 3: Protect stored cardholder data			
3	In its entirety	Customer	Customer is responsible for protecting its cardholder data.
Requirement 4: Encrypt transmission of cardholder data across open, public networks			
4	In its entirety ***Note:*** *SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2 of the PCI Data Security Standard.*	Shared	Customer is responsible for encrypting transmissions of cardholder data across open, public networks and for ensuring it does not use voicemail/call recording for cardholder data. Company's hosted solution is responsible for turning off relaying at Customer's request, and all voice mail must be accessed via telephone user interface (TUI), which also requires a password. The third-party hosting provider encrypts all off-net connections.
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM			
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs			
5.1	Anti-virus software is deployed on all systems commonly affected by malicious software	Shared	Customer and Company are responsible for the own environment.
5.1.1	Anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits)	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
5.1.2	Periodic evaluations are 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	Shared	Customer and Company are responsible for the own environment.
5.2	All anti-virus mechanisms are maintained as follows:		
	(a) All anti-virus software and definitions are kept current	Shared	Customer and Company are responsible for the own environment.
	(b) Automatic updates and periodic scans are enabled and being performed	Shared	Customer and Company are responsible for the own environment.
	(c) All anti-virus mechanisms are generating audit logs, and are logs retained in accordance with PCI-DSS Requirement 10.7	Shared	Customer and Company are responsible for the own environment.
5.3	All anti-virus mechanisms are: • Actively running • Unable to be disabled or altered by users ***Note:*** *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.*	Shared	Customer and Company are responsible for the own environment.
5.4	Security policies and operational procedures for protecting systems against malware are: • Documented • In use • Known to all affected parties	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
Requirement 6: Develop and maintain secure systems and applications			
6.1	A process to identify security vulnerabilities, including the following: • Using reputable outside sources for vulnerability information • Assigning a risk ranking to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities ***Note**: 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.* *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 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.*	Shared	Customer and Company are responsible for the own environment.
6.2	(a) All system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches	Shared	Customer and Company are responsible for the own environment.
	(b) Critical security patches are installed within one month of release ***Note**: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
6.3	(a) Software- development processes are based on industry standards and/or best practices	Shared	Customer and Company are responsible for the own environment.
	(b) Information security is included throughout the software-development life cycle	Shared	Customer and Company are responsible for the own environment.
	(c) Software applications are developed in accordance with PCI- DSS (for example, secure authentication and logging)	Shared	Customer and Company are responsible for the own environment.
	(d) Software development processes ensure the following at 6.3.1 - 6.3.2:	Shared	Customer and Company are responsible for the own environment.
6.3.1	Development, test, and/or custom application accounts, user IDs, and passwords are removed before applications become active or are released to Customers	Shared	Customer and Company are responsible for the own environment. Customers manage all passwords and access to the service.
6.3.2	All custom code is reviewed prior to release to production or Customers to identify any potential coding vulnerability (using either manual or automated processes as follows: • Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable about code review techniques and secure coding practices • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release • Code review results are reviewed and approved by management prior to release ***Note**: 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.*	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
6.4	Change control processes and procedures are followed for all changes to system components to include the following:	Shared	Customer and Company are responsible for the own environment.
6.4.1	(a) Development/test environments are separated from the production environment	Shared	Customer and Company are responsible for the own environment.
	(b) Access control is in place to enforce the separation between the development/test environments and the production environment	Shared	Customer and Company are responsible for the own environment.
6.4.2	The separation of duties between personnel is assigned to the development/test environments and those assigned to the production environment	Shared	Customer and Company are responsible for the own environment.
6.4.3	Production data (live PANs) is ***not*** used for testing or development	Shared	Customer and Company are responsible for the own environment.
6.4.4	Test data and accounts are removed from system components before the system becomes active / goes into production	Shared	Customer and Company are responsible for the own environment.
6.4.5	(a) Change-control procedures are documented and require the following (b) Documentation of impact (c) Documented change control approval by authorized parties (d) Functionality testing to verify that the change does not adversely impact the security of the system (e) Back-out procedures (f) The following are performed and documented for all changes:	Shared	Customer and Company are responsible for the own environment.
6.4.5.1	Documentation of impact	Shared	Customer and Company are responsible for the own environment.
6.4.5.2	Documented approval by authorized parties	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
6.4.5.3	(a) Functionality testing to verify that the change does not adversely impact the security of the system (b) For custom code changes, testing of updates for compliance with PCI-DSS Requirement 6.5 before being deployed into production	Shared	Customer and Company are responsible for the own environment.
6.4.5.4	Back-out procedures	Shared	Customer and Company are responsible for the own environment.
6.4.6	Upon completion of a significant change, are all relevant PCI-DSS requirements implemented on all new or changed systems and networks, and documentation updated as applicable	Shared	Customer and Company are responsible for the own environment.
6.5	(a) Software-development processes address common coding vulnerabilities	Shared	Customer and Company are responsible for the own environment.
	(b) Developers are trained at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities	Shared	Customer and Company are responsible for the own environment.
	(c) Applications are developed based on secure coding guidelines to protect applications from, at a minimum, the following vulnerabilities: ***Note:*** *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 update d (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.*	Shared	Customer and Company are responsible for the own environment.
6.5.1	Coding techniques address injection flaws, particularly SQL injection ***Note:*** *Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.*	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
6.5.2	Coding techniques address buffer overflow vulnerabilities	Shared	Customer and Company are responsible for the own environment.
6.5.3	Coding techniques address insecure cryptographic storage	Shared	Customer and Company are responsible for the own environment.
6.5.4	Coding techniques address insecure communications	Shared	Customer and Company are responsible for the own environment.
6.5.5	Coding techniques address improper error handling	Shared	Customer and Company are responsible for the own environment.
6.5.6	Coding techniques address all “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI-DSS Requirement 6.1)	Shared	Customer and Company are responsible for the own environment.
6.5.7	Coding techniques address cross-site scripting (XSS) vulnerabilities	Shared	Customer and Company are responsible for the own environment.
6.5.8	Coding techniques address improper access control such as insecure direct object references, failure to restrict URL access, directory transversal, and failure to restrict user access to functions.	Shared	Customer and Company are responsible for the own environment.
6.5.9	Coding techniques address cross-site request forgery (CSRF)	Shared	Customer and Company are responsible for the own environment.
6.5.10	Coding techniques address broken authentication and session management	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
6.6	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis, and are these applications protected against known attacks by applying *either* of the following methods • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows: – At least annually – After any changes – By an organization that specializes in application security – That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections ***Note**: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* **– OR –** • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) as follows: – Is situated in front of public-facing web applications to detect and prevent web-based attack – Is actively running and up to date as applicable – Is generating audit logs – Is configured to either block web-based attacks, or generate an alert that is immediately investigated	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
6.7	Security policies and operational procedures for developing and maintaining secure systems and applications are: • Documented • In use • Known to all affected parties		
IMPLEMENT STRONG ACCESS CONTROL MEASURES			
Requirement 7: Restrict access to cardholder data by business need to know			
7.1	Access to system components and cardholder data are limited to only those individuals whose jobs require such access, as follows:	Shared	Customer and Company are responsible for the own environment.
	• A written policy for access control that incorporates the following: – Defining access needs and privilege assignments for each role – Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities, – Assignment of access based on individual personnel's job classification and function – Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved	Shared	Customer and Company are responsible for the own environment.
7.1.1	Access needs for each role are defined, including: • System components and data resources that each role needs to access for the job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources	Shared	Customer and Company are responsible for the own environment.
7.1.2	Access to privileged user IDs is restricted as follows: • To least privileges necessary to perform job responsibilities • Assigned only to roles that specifically require that privileged access	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
7.1.3	Access is assigned based on individual personnel's job classification and function	Shared	Customer and Company are responsible for the own environment.
7.1.4	Documented approval by authorized parties is required, specifying required privileges	Shared	Customer and Company are responsible for the own environment.
7.2	An access control system(s) is 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:	Shared	Customer and Company are responsible for the own environment.
7.2.1	The access control system(s) is in place on all system components	Shared	Customer and Company are responsible for the own environment.
7.2.2	The access control system(s) is configured to enforce privileges assigned to individuals based on job classification and function	Shared	Customer and Company are responsible for the own environment.
7.2.3	The access control system(s) has a default "deny-all" setting	Shared	Customer and Company are responsible for the own environment.
7.3	Security policies and operational procedures for restricting access to cardholder data are: • Documented • In use • Known to all affected parties	Customer	Customer is responsible for its own environment and all cardholder data.
Requirement 8: Identify and authenticate access to system components			
8.1	Policies and procedures for user identification management controls are defined and in place for non-consumer users and administrators on all system components, as follows:	Shared	Customer and Company are responsible for the own environment.
8.1.1	All users are assigned a unique ID before allowing them to access system components or cardholder data	Shared	Customer and Company are responsible for the own environment.
8.1.2	Additions, deletions, and modifications of user IDs, credentials, and other identifier objects are controlled such that user IDs are implemented only as authorized (including with specified privileges)	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
8.1.3	Access for any terminated users are immediately deactivated or removed	Shared	Customer and Company are responsible for the own environment.
8.1.4	Inactive user accounts are either removed or disabled within 90 days	Shared	Customer and Company are responsible for the own environment.
8.1.5	(a) Accounts used by third parties to access, support, or maintain system components via remote access are enabled only during the time period needed and disabled when not in use	Shared	Customer and Company are responsible for the own environment.
	(b) Third party remote access accounts are monitored when in use	Shared	Customer and Company are responsible for the own environment.
8.1.6	(a) Repeated access attempts are limited by locking out the user ID after no more than six attempts	Shared	Customer and Company are responsible for the own environment.
	(b) *For service providers only*: Non-consumer Customer passwords are temporarily locked-out after not more than six invalid access attempts	Shared	Customer and Company are responsible for the own environment.
8.1.7	Once a user account is locked out, the lockout duration is set to a minimum of 30 minutes or until an administrator enables the user ID	Shared	Customer and Company are responsible for the own environment.
8.1.8	If a session has been idle for more than 15 minutes, users are required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session	Shared	Customer and Company are responsible for the own environment.
8.2	In addition to assigning a unique ID, one or more of the following methods are employed to authenticate all users • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric	Shared	Customer and Company are responsible for the own environment.
8.2.1	(a) Strong cryptography is used to render all authentication credentials (such as passwords/passphrases) unreadable during transmission and storage on all system components	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) *For service providers only*: Strong cryptography is used to render all non-consumer Customers' authentication credentials (such as passwords/passphrases) unreadable during transmission and storage on all system components	Shared	Customer and Company are responsible for the own environment.
8.2.2	User identity is verified before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys)	Shared	Customer and Company are responsible for the own environment.
8.2.3	(a) User password parameters are configured to require passwords/passphrases meet the following: • A minimum password length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	Shared	Customer and Company are responsible for the own environment.
	(b) *For service providers only:* Non-consumer Customer passwords are required to meet the following minimum length and complexity requirements • A minimum password length of at least seven characters • Contain both numeric and alphabetic characters	Shared	Customer and Company are responsible for the own environment.
8.2.4	(a) User passwords/passphrases are changed at least once every 90 days	Shared	Customer and Company are responsible for the own environment.
	(b) *For service providers only*: Non-consumer Customer passwords are required to be changed periodically, and non- consumer Customers are given guidance as to when, and under what circumstances, passwords must change.	Shared	Customer and Company are responsible for the own environment.
8.2.5	(a) An individual must submit a new password/passphrase that is different from any of the last four passwords/passphrases he or she has used	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) *For service providers only*: New, non-consumer Customer passwords are required to be different from any of the last four passwords used	Shared	Customer and Company are responsible for the own environment.
8.2.6	Passwords/passphrases are set to a unique value for each user for first-time use and upon reset, and must each user change the password immediately after the first use	Shared	Customer and Company are responsible for the own environment.
8.3	All individual non-console administrative access and all remote access to the CDE is secured using multi-factor authentication, as follows: ***Note:*** *Multi-factor authentication requires that a minimum of 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 multi-factor authentication.*	Customer	Customer is fully responsible for the CDE. Company and its vendors do not have access to voice mailbox contents.
8.3.1	Multi-factor authentication is incorporated for all non-console access into the CDE for personnel with administrative access	Customer	Customer is responsible for the CDE.
8.3.2	Multi-factor authentication is incorporated for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network	Shared	Customer and Company are responsible for the own environment.
8.4	(a) Authentication policies and procedures are documented and communicated to all users	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) Authentication policies and procedures include the following: • Guidance on selecting strong authentication credentials • Guidance for how users should protect the authentication credentials • Instructions not to reuse previously used passwords • Instructions that users should change passwords if there is any suspicion the password could be compromised	Shared	Customer and Company are responsible for the own environment.
8.5	Group, shared, or generic accounts, passwords, or other authentication methods are prohibited as follows: • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system components	Shared	Customer and Company are responsible for the own environment.
8.5.1	*For service providers only*: 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/passphrase) for each Customer ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing the own hosting environment, where multiple Customer environments are hosted.*	Company	Unique authentication credentials for access to each Customer premise are used by Company.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, and certificates, etc.), the use of these mechanisms is assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	Shared	Customer and Company are responsible for the own environment.
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:	Customer	Customer is responsible for all cardholder data.
	(a) All user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures)	Customer	Customer is responsible for the CDE.
	(b) User direct access to or queries of databases are restricted to database administrators	Customer	Customer is responsible for the CDE.
	(c) Application IDs are only able to be used by the applications (and not by individual users or other processes)	Customer	Customer is responsible for the CDE.
8.8	Security policies and operational procedures for identification and authentication are: • Documented • In use • Known to all affected parties	Customer	Customer is responsible for the CDE.
Requirement 9: Restrict physical access to cardholder data			
9.1	Appropriate facility entry controls are in place to limit and monitor physical access to systems in the CDE	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
9.1.1	(a) Either video cameras or access-control mechanisms (or both) are in place to monitor individual physical access to sensitive areas ***Note:*** *"Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present such as the cashier areas in a retail store.*	Customer	Customer is responsible for the CDE.
	(b) Either video cameras or access-control mechanisms (or both) are protected from tampering or disabling	Customer	Customer is responsible for the CDE.
	(c) Data collected from video cameras and/or access control mechanisms is reviewed and correlated with other entries	Customer	Customer is responsible for the CDE.
	(d) Data collected from video cameras and/or access control mechanisms is stored for at least three months unless otherwise restricted by law	Customer	Customer is responsible for the CDE.
9.1.2	Physical and/or logical controls are in place to restrict access to publicly accessible network jacks *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.*	Customer	Customer is responsible for the CDE.
9.1.3	Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines are restricted	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
9.2	(a) Procedures are developed to easily distinguish between onsite personnel and visitors, which include: • Identifying onsite personnel and visitors (for example, assigning badges), • Changing access requirements, and • Revoking terminated onsite personnel and expired visitor identification (such as ID badges) *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.*	Customer	Customer is responsible for the CDE.
	(b) Identification methods (such as ID badges) clearly identify visitors and easily distinguish between onsite personnel and visitors	Customer	Customer is responsible for the CDE.
	(c) Access to the badge system is limited to authorized personnel	Customer	Customer is responsible for the CDE.
9.3	Physical access to sensitive areas is controlled for onsite personnel, as follows: • Access is authorized and based on individual job function • Access is revoked immediately upon termination • Upon termination, all physical access mechanisms, such as keys, access cards, etc., are returned or disabled	Customer	Customer is responsible for the CDE.
9.4	Visitor identification and access are handled as follows:	Customer	Customer is responsible for the CDE.
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
9.4.2	(a) Visitors are identified and given a badge or other identification that visibly distinguishes the visitors from onsite personnel	Customer	Customer is responsible for the CDE.
	(b) Visitor badges or other identification expire	Customer	Customer is responsible for the CDE.
9.4.3	Visitors are asked to surrender the badge or other identification before leaving the facility or at the date of expiration	Customer	Customer is responsible for the CDE.
9.4.4	(a) A visitor log is 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	Customer	Customer is responsible for the CDE.
	(b) The visitor log contains the visitor's name, the firm represented, and the onsite personnel authorizing physical access	Customer	Customer is responsible for the CDE.
	(c) The visitor log is retained for at least three months	Customer	Customer is responsible for the CDE.
9.5	All media is physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes) *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*	Customer	Customer is responsible for the CDE.
9.5.1	The location where media back-ups are stored is reviewed at least annually to confirm storage is secure	Customer	Customer is responsible for the CDE.
9.6	(a) Strict control is maintained over the internal or external distribution of any kind of media	Customer	Customer is responsible for the CDE.
	(b) Controls include the following:	Customer	Customer is responsible for the CDE.
9.6.1	Media is classified so the sensitivity of the data can be determined	Customer	Customer is responsible for the CDE.
9.6.2	Media is sent by secured courier or other delivery method that can be accurately tracked	Customer	Customer is responsible for the CDE.
9.6.3	Management approval is obtained prior to moving the media (especially when media is distributed to individuals)	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
9.7	Strict control is maintained over the storage and accessibility of media	Customer	Customer is responsible for the CDE.
9.7.1	(a) Inventory logs of all media are properly maintained	Customer	Customer is responsible for the CDE.
	(b) Periodic media inventories are conducted at least annually	Customer	Customer is responsible for the CDE.
9.8	(a) Media is destroyed when it is no longer needed for business or legal reasons	Customer	Customer is responsible for the CDE.
	(b) A periodic media destruction policy that defines requirements for the following: • Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. • Storage containers used for materials that are to be destroyed must be secured. • Cardholder data on electronic media must be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	Customer	Customer is responsible for the CDE.
	(c) Media destruction is performed as follows:	Customer	Customer is responsible for the CDE.
9.8.1	(a) Hardcopy materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed	Customer	Customer is responsible for the CDE.
	(b) Storage containers are used for materials that contain information to be destroyed secured to prevent access to the contents	Customer	Customer is responsible for the CDE.
9.8.2	Cardholder data on electronic media is rendered unrecoverable (e.g. 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	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
9.9	Devices that capture payment card data via direct physical interaction with the card are protected against tampering and substitution as follows ***Note:*** *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.*	Customer	Customer is responsible for the CDE.
	(a) Policies and procedures require that a list of such devices be maintained	Customer	Customer is responsible for the CDE.
	(b) Policies and procedures require that devices are periodically inspected to look for tampering or substitution	Customer	Customer is responsible for the CDE.
	(c) Policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices	Customer	Customer is responsible for the CDE.
9.9.1	(a) The list of devices includes the following • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification	Customer	Customer is responsible for the CDE.
	(b) The list is accurate and up to date	Customer	Customer is responsible for the CDE.
	(c) The list of devices is updated when devices are added, relocated, decommissioned, etc.	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
9.9.2	(a) Device surfaces are 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 ***Note:*** *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.*	Customer	Customer is responsible for the CDE.
	(b) Personnel are aware of procedures for inspecting devices	Customer	Customer is responsible for the CDE.
9.9.3	Personnel are trained to be aware of attempted tampering or replacement of devices, to include the following:	Customer	Customer is responsible for the CDE.
	(a) Training materials for personnel are at point-of-sale locations include the following • 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. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Customer	Customer is responsible for the CDE.
	(b) Personnel at point-of-sale locations have received training, and are they aware of procedures to detect and report attempted tampering or replacement of devices	Customer	Customer is responsible for the CDE.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
9.10	Security policies and operational procedures for restricting physical access to cardholder data are: • Documented • In use • Known to all affected parties	Customer	Customer is responsible for the CDE.
REGULARLY MONITOR AND TEST NETWORKS			
Requirement 10: Track and monitor all access to network resources and cardholder data			
10.1	(a) Audit trails are enabled and active for system components	Shared	Customer and Company are responsible for the own environment.
	(b) Access to system components is linked to individual users	Shared	Customer and Company are responsible for the own environment.
10.2	Automated audit trails are implemented for all system components to reconstruct the following events:	Shared	Customer and Company are responsible for the own environment.
10.2.1	All individual user accesses to cardholder data	Shared	Customer and Company are responsible for the own environment.
10.2.2	All actions taken by any individual with root or administrative privileges	Shared	Customer and Company are responsible for the own environment.
10.2.3	Access to all audit trails	Shared	Customer and Company are responsible for the own environment.
10.2.4	Invalid logical access attempts	Shared	Customer and Company are responsible for the own environment.
10.2.5	Identification and authentication mechanisms exist – 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	Shared	Customer and Company are responsible for the own environment.
10.2.6	Initialization, stopping, or pausing of the audit logs	Shared	Customer and Company are responsible for the own environment.
10.2.7	Creation and deletion of system-level objects	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
10.3	The following audit trail entries are recorded for all system components for each event:		
10.3.1	User identification	Shared	Customer and Company are responsible for the own environment.
10.3.2	Type of event	Shared	Customer and Company are responsible for the own environment.
10.3.3	Date and time	Shared	Customer and Company are responsible for the own environment.
10.3.4	Success or failure indication	Shared	Customer and Company are responsible for the own environment.
10.3.5	Origination of event	Shared	Customer and Company are responsible for the own environment.
10.3.6	Identity or name of affected data, system component, or resource	Shared	Customer and Company are responsible for the own environment.
10.4	All critical system clocks and times are synchronized through use of time synchronization technology, and is the technology kept current ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	Shared	Customer and Company are responsible for the own environment.
10.4.1	The following processes are implemented for critical systems to have the correct and consistent time:		
	(a) Only designated central time server(s) receive time signals from external sources, and time signals are from external sources based on International Atomic Time or UTC	Shared	Customer and Company are responsible for the own environment.
	(b) Where there is more than one designated time server, the time servers peer with each other to keep accurate time	Shared	Customer and Company are responsible for the own environment.
	(c) Systems receive time only from designated central time server(s)	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
10.4.2	Time data is protected as follows: (a) Access to time data is restricted to only personnel with a business need to access time data	Shared	Customer and Company are responsible for the own environment.
	(b) Changes to time settings on critical systems are logged, monitored, and reviewed	Shared	Customer and Company are responsible for the own environment.
10.4.3	Time settings are received from specific, industry-accepted time sources (This is to prevent a malicious individual from changing the clock). *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).*	Shared	Customer and Company are responsible for the own environment.
10.5	Audit trails are secured so they cannot be altered, as follows:	Shared	Customer and Company are responsible for the own environment.
10.5.1	Viewing of audit trails is limited to those with a job-related need	Shared	Customer and Company are responsible for the own environment.
10.5.2	Audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation	Shared	Customer and Company are responsible for the own environment.
10.5.3	Audit trail files are promptly backed up to a centralized log server or media that is difficult to alter	Shared	Customer and Company are responsible for the own environment.
10.5.4	Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media	Shared	Customer and Company are responsible for the own environment.
10.5.5	File-integrity monitoring or change-detection software used on logs is to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
10.6	Logs and security events for all system components are reviewed to identify anomalies or suspicious activity as follows: ***Note:*** *Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.*	Shared	Customer and Company are responsible for the own environment.
10.6.1	(a) Written policies and procedures are 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 • 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.)	Shared	Customer and Company are responsible for the own environment.
	(b) The above logs and security events are reviewed at least daily	Shared	Customer and Company are responsible for the own environment.
10.6.2	(a) Written policies and procedures are 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	Shared	Customer and Company are responsible for the own environment.
	(b) Reviews of all other system components are performed in accordance with organization's policies and risk management strategy	Shared	Customer and Company are responsible for the own environment.
10.6.3	(a) Written policies and procedures are defined for following up on exceptions and anomalies identified during the review process	Shared	Customer and Company are responsible for the own environment.
	(b) Follow up to exceptions and anomalies are performed	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
10.7	(a) Audit log retention policies and procedures are 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)	Shared	Customer and Company are responsible for the own environment.
	(b) Audit logs are retained for at least one year	Shared	Customer and Company are responsible for the own environment.
	(c) At least the last three months' logs are immediately available for analysis	Shared	Customer and Company are responsible for the own environment.
10.8	*For service providers only*: Is a process implemented for the timely detection and reporting of failures of critical security control systems as follows:	N/A	N/A
	(a) Processes are implemented for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used)	Company	Company is responsible for implementing and documenting a process for the timely detection, alerting, reporting, and responding to failures of critical security control systems.
	(b) The failure of a critical security control results in the generation of an alert	Company	Company is responsible for implementing and documenting a process for the timely detection, alerting, reporting, and responding to failures of critical security control systems.
10.8.1	*For service providers only*: Failures of any critical security controls are responded to in a timely manner, as follows:	Company	Company is responsible for implementing and documenting a process for the timely detection, alerting, reporting, and responding to failures of critical security control systems.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(a) Processes for responding to critical security control failures are defined and implemented, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls	Company	Company is responsible for implementing and documenting a process for the timely detection, alerting, reporting, and responding to failures of critical security control systems.
	(b) Failures in critical security controls are documented, including: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	Company	Company is responsible for implementing and documenting a process for the timely detection, alerting, reporting, and responding to failures of critical security control systems.
10.9	Security policies and operational procedures exist for monitoring all access to network resources and cardholder data: • Documented • In use • Known to all affected parties	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
Requirement 11: Regularly test security systems and processes			
11.1	(a) Processes are implemented for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis ***Note:*** *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. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	Shared	Customer and Company are responsible for the own environment.
	(a) The methodology detects and identifies any unauthorized wireless access points, including at least the following: • WLAN cards inserted into system components; • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.); and • Wireless devices attached to a network port or network device.	Shared	Customer and Company are responsible for the own environment.
	(b) If wireless scanning is utilized to identify authorized and unauthorized wireless access points, the scan is performed at least quarterly for all system components and facilities	Shared	Customer and Company are responsible for the own environment.
	(c) If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), monitoring is configured to generate alerts to notify personnel	Shared	Customer and Company are responsible for the own environment.
11.1.1	An inventory of authorized wireless access points is maintained, and a business justification documented for all authorized wireless access points	Shared	Customer and Company are responsible for the own environment.
11.1.2	(a) The incident response plan is defined and requires a response in the event that an unauthorized wireless access point is detected	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) Action is taken when unauthorized wireless access points are found	Shared	Customer and Company are responsible for the own environment.
11.2	Internal and external network vulnerability scans are 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: ***Note:*** *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.* *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.*	Shared	Customer and Company are responsible for the own environment.
11.2.1	(a) Quarterly internal vulnerability scans are performed	Shared	Customer and Company are responsible for the own environment.
	(b) The quarterly internal scan process addresses all “high risk” vulnerabilities and includes rescans to verify all “high-risk” vulnerabilities (as defined in PCI-DSS Requirement 6.1) are resolved	Shared	Customer and Company are responsible for the own environment.
	(c) Quarterly internal scans are performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV)	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
11.2.2	(a) Quarterly external vulnerability scans are performed ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan Customer responsibilities, scan preparation, etc.*	Shared	Customer and Company are responsible for the own environment.
	(b) External quarterly scans 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)	Shared	Customer and Company are responsible for the own environment.
	(c) Quarterly external vulnerability scans are performed by a PCI SSC Approved Scanning Vendor (ASV)	Shared	Customer and Company are responsible for the own environment.
11.2.3	(a) Internal and external scans, and rescans as needed, are performed after any significant change ***Note:*** *Scans must be performed by qualified personnel.*	Shared	Customer and Company are responsible for the own environment.
	(b) The scan process includes 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	Shared	Customer and Company are responsible for the own environment.
	(c) Scans are 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)	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
11.3	The penetration-testing methodology includes 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	Shared	Customer and Company are responsible for the own environment.
11.3.1	(a) *External* penetration testing is 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)	Shared	Customer and Company are responsible for the own environment.
	(b) Tests are 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)	Shared	Customer and Company are responsible for the own environment.
11.3.2	(a) *Internal* penetration testing is 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)	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) Tests are 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)	Shared	Customer and Company are responsible for the own environment.
11.3.3	Exploitable vulnerabilities found during penetration testing corrected, followed by repeated testing to verify the corrections	Shared	Customer and Company are responsible for the own environment.
11.3.4	If segmentation is used to isolate the CDE from other networks:	Shared	Customer and Company are responsible for the own environment.
	(a) Penetration-testing procedures are defined to test all segmentation methods, to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE	Shared	Customer and Company are responsible for the own environment.
	(b) Penetration testing verifies segmentation controls to meet the following • Performed at least annually and after any changes to segmentation controls/methods • Covers all segmentation controls/methods in use • Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Shared	Customer and Company are responsible for the own environment.
	(c) Tests are 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)	Shared	Customer and Company are responsible for the own environment.
11.3.4.1	*For service providers only:* If segmentation is used:	Shared	Customer and Company are responsible for the own environment.
	(a) PCI-DSS scope is confirmed by performing penetration tests on segmentation controls at least every six months and after any changes to segmentation controls/methods	Shared	Customer and Company are responsible for the own environment.
	(b) Penetration testing covers all segmentation controls/methods in use	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(c) Penetration testing verifies that segmentation controls/methods are operational and effective, and isolates all out-of-scope systems from systems in the CDE	Shared	Customer and Company are responsible for the own environment.
	(d) Tests are 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)	Shared	Customer and Company are responsible for the own environment.
11.4	(a) Intrusion-detection and/or intrusion-prevention techniques that detect and/or prevent intrusions into the network in place to monitor all traffic: • At the perimeter of the CDE, and • At critical points in the CDE.	Shared	Customer and Company are responsible for the own environment.
	(b) Intrusion-detection and/or intrusion-prevention techniques configured to alert personnel of suspected compromises	Shared	Customer and Company are responsible for the own environment.
	(c) All intrusion-detection and prevention engines, baselines, and signatures kept up-to-date	Shared	Customer and Company are responsible for the own environment.
11.5	(a) A change-detection mechanism (for example, file-integrity monitoring tools) is deployed to detect unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files Examples of files that should be monitored include: • *System executables* • *Application executables* • *Configuration and parameter files* • *Centrally stored, historical or archived, log, and audit files* • *Additional critical files determined by entity (for example, through risk assessment or other means)*	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) The change-detection mechanism is 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 ***Note:*** *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.*	Shared	Customer and Company are responsible for the own environment.
11.5.1	A process is in place to respond to any alerts generated by the change-detection solution	Shared	Customer and Company are responsible for the own environment.
11.6	Security policies and operational procedures are for security monitoring and testing: ▪ Documented ▪ In use ▪ Known to all affected parties	Shared	Customer and Company are responsible for the own environment.
MAINTAIN AN INFORMATION SECURITY POLICY			
Requirement 12: Maintain a policy that addresses information security for all personnel			
12.1	A security policy is established, published, maintained, and disseminated to all relevant personnel	Shared	Customer and Company are responsible for the own environment.
12.1.1	The security policy is reviewed at least annually and updated when the environment changes	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
12.2	(a) An annual risk assessment process is implemented that: • Identifies critical assets, threats, and vulnerabilities, AND • Results in a formal, documented analysis of risk *Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.*	Shared	Customer and Company are responsible for the own environment.
	(b) The risk assessment process is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.)	Shared	Customer and Company are responsible for the own environment.
12.3	Usage policies for critical technologies developed to define proper use of these technologies and require the following: ***Note:*** *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.*	Shared	Customer and Company are responsible for the own environment.
12.3.1	Explicit approval by authorized parties to use the technologies	Shared	Customer and Company are responsible for the own environment.
12.3.2	Authentication for use of the technology	Shared	Customer and Company are responsible for the own environment.
12.3.3	A list of all such devices and personnel with access	Shared	Customer and Company are responsible for the own environment.
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	Shared	Customer and Company are responsible for the own environment.
12.3.5	Acceptable uses of the technologies	Shared	Customer and Company are responsible for the own environment.
12.3.6	Acceptable network locations for the technologies	Shared	Customer and Company are responsible for the own environment.
12.3.7	List of Company-approved products	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Shared	Customer and Company are responsible for the own environment.
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	Shared	Customer and Company are responsible for the own environment.
12.3.10	(a) 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 *Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI-DSS Requirements.*	Shared	Customer and Company are responsible for the own environment.
	(b) For personnel with proper authorization, the policy requires the protection of cardholder data in accordance with PCI-DSS Requirements	Shared	Customer and Company are responsible for the own environment.
12.4	Security policy and procedures clearly define information security responsibilities for all personnel	Shared	Customer and Company are responsible for the own environment.
12.4.1	*For service providers only*: Executive management have established responsibility for the protection of cardholder data and a PCI-DSS compliance program, as follows:	Shared	Customer and Company are responsible for the own environment.
	(a) Executive management has assigned overall accountability for maintaining the entity's PCI-DSS compliance	Shared	Customer and Company are responsible for the own environment.
	(b) Executive management has defined a charter for the PCI-DSS compliance program and communication to executive management	Shared	Customer and Company are responsible for the own environment.
12.5	(a) Responsibility for information security is formally assigned to a Chief Security Officer or other security-knowledgeable member of management	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) The following information security management responsibilities are formally assigned to an individual or team:	Shared	Customer and Company are responsible for the own environment.
12.5.1	Establishing, documenting, and distributing security policies and procedures	Shared	Customer and Company are responsible for the own environment.
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel	Shared	Customer and Company are responsible for the own environment.
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations	Shared	Customer and Company are responsible for the own environment.
12.5.4	Administering user accounts, including additions, deletions, and modifications	Shared	Customer and Company are responsible for the own environment.
12.5.5	Monitoring and controlling all access to data	Shared	Customer and Company are responsible for the own environment.
12.6	(a) A formal security awareness program is in place to make all personnel aware of the cardholder data security policy and procedures	Shared	Customer and Company are responsible for the own environment.
	(b) Security awareness program procedures include the following:	Shared	Customer and Company are responsible for the own environment.
12.6.1	(a) The security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions) ***Note:*** *Methods can vary depending on the role of the personnel and the level of access to the cardholder data.*	Shared	Customer and Company are responsible for the own environment.
	(b) Personnel are educated upon hire and at least annually	Shared	Customer and Company are responsible for the own environment.
	(c) Employees completed awareness training and they are aware of the importance of cardholder data security	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
12.6.2	Personnel are required to acknowledge at least annually that they have read and understood the security policy and procedures	Shared	Customer and Company are responsible for the own environment.
12.7	Potential personnel (see definition of "personnel" above) are screened prior to hire to minimize the risk of attacks from internal sources *Examples of background checks include previous employment history, criminal record, credit history and reference checks.* ***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.*	Shared	Customer and Company are responsible for the own environment.
12.8	Policies and procedures are maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	Shared	Customer and Company are responsible for the own environment.
12.8.1	A list of service providers is maintained, including a description of the service(s) provided	Shared	Customer and Company are responsible for the own environment.
12.8.2	A written agreement is 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 CDE ***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.*	Shared	Customer and Company are responsible for the own environment.
12.8.3	An established process for engaging service providers, including proper due diligence prior to engagement	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
12.8.4	A program is maintained to monitor service providers' PCI-DSS compliance status at least annually	Shared	Customer and Company are responsible for the own environment.
12.8.5	Information is maintained about which PCI-DSS requirements are managed by each service provider, and which are managed by the entity	Shared	Customer and Company are responsible for the own environment.
12.9	*For service providers only*: 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 CDE ***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.*	Company	Company acknowledges in writing to Customers that Customers are responsible for the security of the 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 CDE.
12.10	An incident response plan has been implemented in preparation to respond immediately to a system breach, as follows:	Shared	Customer and Company are responsible for the own environment.
12.10.1	(a) An incident response plan been created to be implemented in the event of system breach	Shared	Customer and Company are responsible for the own environment.

PCI SECTION NO.	REQUIREMENT	RESPONSIBILITY	DETAILS
	(b) The plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands	Shared	Customer and Company are responsible for the own environment.
12.10.2	The plan is reviewed and tested at least annually, including all elements listed in Requirement 12.10.1	Shared	Customer and Company are responsible for the own environment.
12.10.3	Specific personnel are designated to be available on a 24/7 basis to respond to alerts	Shared	Customer and Company are responsible for the own environment.
12.10.4	Appropriate training is provided to staff with security breach response responsibilities	Shared	Customer and Company are responsible for the own environment.
12.10.5	Alerts from security monitoring systems are included in the incident response plan	Shared	Customer and Company are responsible for the own environment.
12.10.6	A process is developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments	Shared	Customer and Company are responsible for the own environment.