PCI DSS Question		Response		
		Yes	No	N/A
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:			
7.1.a	Is there 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	☑	☐	
7.1.1	Are access needs for each role defined, including: * System components and data resources that each role needs to access for their job function? * Level of privilege required (for example, user, administrator, etc.) for accessing resources?	☑	☐	
7.1.2	Is access to privileged user IDs restricted as follows: * To least privileges necessary to perform job responsibilities? * Assigned only to roles that specifically require that privileged access?	☑	☐	
7.1.3	Is access assigned based on individual personnel's job classification and function?	☑	☐	
7.1.4	Is documented approval by authorized parties required, specifying required privileges?	☑	☐	
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	Is the access control system(s) in place on all system components?	☑	☐	
7.2.2	Is the access control system(s) configured to enforce privileges assigned to individuals based on job classification and function?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
7.2.3	Does the access control system(s) have a default "deny-all" setting?	☑	☐	
7.3	Are security policies and operational procedures for restricting access to cardholder data: * Documented * In use * Known to all affected parties?	☑	☐	

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Response		
		Yes	No	N/A
8.1	Are policies and procedures for user identification management controls defined and in place for non-consumer users and administrators on all system components, as follows:			
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	☑	☐	
8.1.2	Are additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled such that user IDs are implemented only as authorized (including with specified privileges)?	☑	☐	
8.1.3	Is access for any terminated users immediately deactivated or removed?	☑	☐	
8.1.4	Are inactive user accounts either removed or disabled within 90 days?	☑	☐	
8.1.5.a	Are accounts used by third parties to access, support, or maintain system components via remote access enabled only during the time period needed and disabled when not in use?	☑	☐	
8.1.5.b	Are third party remote access accounts monitored when in use?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
8.1.6.a	Are repeated access attempts limited by locking out the user ID after no more than six attempts?	☑	☐	
8.1.7	Once a user account is locked out, is the lockout duration set to a minimum of 30 minutes or until an administrator enables the user ID?	☑	☐	
8.1.8	If a session has been idle for more than 15 minutes, are users required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session?	☑	☐	
8.2	In addition to assigning a unique ID, is one or more of the following methods 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	☑	☐	
8.2.1.a	Is strong cryptography used to render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components?	☑	☐	
8.2.2	Is user identity verified before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys)?	☑	☐	
8.2.3.a	Are user password parameters 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/phrases must have complexity and strength at least equivalent to the parameters specified above.	☑	☐	
8.2.4.a	Are user passwords/passphrases changed at least once every 90 days?	☑	☐	
8.2.5.a	Must an individual submit a new password/phrase that is different from any of the last four passwords/phrases he or she has used?	☑	☐	
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?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
8.3	Is all individual non-console administrative access and all remote access to the CDE 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.			
8.3.1	Is multi-factor authentication incorporated for all nonconsole access into the CDE for personnel with administrative access?	☑	☐	
8.3.2	Is multi-factor authentication 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?	☑	☐	
8.4.a	Are authentication procedures and policies documented and communicated to all users?	☑	☐	
8.4.b	Do authentication procedures and policies include the following? * Guidance on selecting strong authentication credentials * Guidance for how users should protect their 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	☑	☐	
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods 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?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
8.6	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? * 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	☑	☐	
8.7	Is all access to any database containing cardholder data (including access by applications, administrators, and all other users) restricted as follows:			
8.7.a	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)?	☑	☐	
8.7.b	Is user direct access to or queries to of databases restricted to database administrators?	☑	☐	
8.7.c	Are application IDs only able to be used by the applications (and not by individual users or other processes)?	☑	☐	
8.8	Are security policies and operational procedures for identification and authentication: * Documented * In use * Known to all affected parties?	☑	☐	

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Response		
		Yes	No	N/A
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	☑	☐	☐

PCI DSS Question		Response		
		Yes	No	N/A
9.1.1.a	Are either video cameras or access-control mechanisms (or both) 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.	☑	☐	☐
9.1.1.b	Are either video cameras or access-control mechanisms (or both) protected from tampering or disabling?	☑	☐	☐
9.1.1.c	Is data collected from video cameras and/or access control mechanisms reviewed and correlated with other entries?	☑	☐	☐
9.1.1.d	Is data collected from video cameras and/or access control mechanisms stored for at least three months unless otherwise restricted by law?	☑	☐	☐
9.1.2	Are physical and/or logical controls 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.	☑	☐	☐
9.1.3	Is physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines restricted?	☑	☐	☐

	PCI DSS Question	Response		
		Yes	No	N/A
9.2.a	Are procedures 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.	☑	☐	☐
9.2.b	Do identification methods (such as ID badges) clearly identify visitors and easily distinguish between onsite personnel and visitors?	☑	☐	☐
9.2.c	Is access to the badge system limited to authorized personnel?	☑	☐	☐
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?	☑	☐	☐
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?	☑	☐	☐
9.4.2.a	Are visitors identified and given a badge or other identification that visibly distinguishes the visitors from onsite personnel?	☑	☐	☐
9.4.2.b	Do visitor badges or other identification expire?	☑	☐	☐
9.4.3	Are visitors asked to surrender the badge or other identification before leaving the facility or at the date of expiration?	☑	☐	☐

PCI DSS Question		Response		
		Yes	No	N/A
9.4.4.a	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?	☑	☐	☐
9.4.4.b	Does the visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access?	☑	☐	☐
9.4.4.c	Is the visitor log retained for at least three months?	☑	☐	☐
9.5	Are all media 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.	☑	☐	
9.5.1	Is the location where media back-ups are stored reviewed at least annually to confirm storage is secure?	☑	☐	
9.6.a	Is strict control maintained over the internal or external distribution of any kind of media?	☑	☐	
9.6.b	Do controls include the following:			
9.6.1	Is media classified so the sensitivity of the data can be determined?	☑	☐	
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	☑	☐	
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	☑	☐	
9.7	Is strict control maintained over the storage and accessibility of media?	☑	☐	
9.7.1.a	Are inventory logs of all media properly maintained?	☑	☐	
9.7.1.b	Are periodic media inventories conducted at least annually?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
9.8.a	Is all media destroyed when it is no longer needed for business or legal reasons?	☑	☐	
9.8.b	Is there 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 via a secure wipe program (in accordance with industry-accepted standards for secure deletion), or by physically destroying the media.	☑	☐	
9.8.c	Is media destruction performed as follows:			
9.8.1.a	Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	☑	☐	
9.8.1.b	Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	☑	☐	
9.8.2	Is cardholder data on electronic media 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?	☑	☐	
9.9	Are devices that capture payment card data via direct physical interaction with the card 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.			
9.9.a	Do policies and procedures require that a list of such devices maintained?	☑	☐	
9.9.b	Do policies and procedures require that devices are periodically inspected to look for tampering or substitution?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
9.9.c	Do policies and procedures require that personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices?	☑	☐	
9.9.1.a	Does the list of devices include 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	☑	☐	
9.9.1.b	Is the list accurate and up to date?	☑	☐	
9.9.1.c	Is the list of devices updated when devices are added, relocated, decommissioned, etc.?	☑	☐	
9.9.2.a	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? 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.	☑	☐	
9.9.2.b	Are personnel aware of procedures for inspecting devices?	☑	☐	
9.9.3	Are personnel trained to be aware of attempted tampering or replacement of devices, to include the following?			
9.9.3.a	Do training materials for personnel 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).	☑	☐	