securityMETRICS®

PCI Security Standards Council®

Payment Card Industry (PCI)

Data Security Standard

Self-Assessment Questionnaire D

All other SAQ-Eligible Merchants

For use with PCI DSS Version 3.2.1

February 2020

Note: The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the PCI DSS Requirements and Security Assessment Procedures document.

Build and Maintain a Secure Network and Systems

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

PCI DSS Question		Response		
		Yes	No	N/A
1.1	Are firewall and router configuration standards established and implemented to include the following:			
1.1.1	Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	☑	☐	
1.1.2.a	Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?	☑	☐	
1.1.2.b	Is there a process to ensure the diagram is kept current?	☑	☐	
1.1.3.a	Is there a current diagram that shows all cardholder data flows across systems and networks?	☑	☐	
1.1.3.b	Is there a process to ensure the diagram is kept current?	☑	☐	
1.1.4.a	Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?	☑	☐	
1.1.4.b	Is the current network diagram consistent with the firewall configuration standards?	☑	☐	
1.1.5	Are groups, roles, and responsibilities for logical management of network components assigned and documented in the firewall and router configuration standards?	☑	☐	
1.1.6.a	Do firewall and router configuration standards include a documented list of services, protocols, and ports, including business justification and approval for each?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
1.1.6.b	Are all insecure services, protocols, and ports identified, and are security features documented and implemented for each identified service?	☑	☐	
1.1.7.a	Do firewall and router configuration standards require review of firewall and router rule sets at least every six months?	☑	☐	
1.1.7.b	Are firewall and router rule sets reviewed at least every six months?	☑	☐	
1.2	Do firewall and router configurations restrict connections between untrusted networks and any system in the cardholder data environment 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.			
1.2.1.a	Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment?	☑	☐	
1.2.1.b	Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?	☑	☐	
1.2.2	Are router configuration files secured from unauthorized access and synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted)?	☑	☐	
1.2.3	Are perimeter firewalls installed between all wireless networks and the cardholder data environment, and are these firewalls configured to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment?	☑	☐	
1.3	Is direct public access prohibited between the Internet and any system component in the cardholder data environment, as follows:			
1.3.1	Is a DMZ implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports?	☑	☐	

	PCI DSS Question	Response		
		Yes	No	N/A
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	☑	☐	
1.3.3	Are anti-spoofing measures implemented to detect and block forged sourced IP addresses from entering the network? (For example, block traffic originating from the internet with an internal address.)	☑	☐	
1.3.4	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	☑	☐	
1.3.5	Are only established connections permitted into the network?	☑	☐	
1.3.6	Are system components that store cardholder data (such as a database) placed in an internal network zone, segregated from the DMZ and other untrusted networks?	☑	☐	
1.3.7.a	Are methods 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.	☑	☐	
1.3.7.b	Is any disclosure of private IP addresses and routing information to external entities authorized?	☑	☐	
1.4.a	Is personal firewall software (or equivalent functionality) 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?	☑	☐	
1.4.b	Is the personal firewall software (or equivalent functionality) configured to specific configuration settings, actively running, and not alterable by users of mobile and/or employee-owned devices?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
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

PCI DSS Question		Response		
		Yes	No	N/A
2.1.a	Are vendor-supplied defaults always changed before installing a system on the network? This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	☑	☐	
2.1.b	Are unnecessary default accounts removed or disabled before installing a system on the network?	☑	☐	
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are ALL wireless vendor defaults changed at installations, as follows:			
2.1.1.a	Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?	☑	☐	☐
2.1.1.b	Are default SNMP community strings on wireless devices changed at installation?	☑	☐	☐
2.1.1.c	Are default passwords/passphrases on access points changed at installation?	☑	☐	☐

PCI DSS Question		Response		
		Yes	No	N/A
2.1.1.d	Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?	☑	☐	☐
2.1.1.e	Are other security-related wireless vendor defaults changed, if applicable?	☑	☐	☐
2.2.a	Are configuration standards developed for all system components and are they consistent with industry-accepted system hardening standards? Sources of industry-accepted system hardening standards may include, but are not limited to, SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), International Organization for Standardization (ISO), and Center for Internet Security (CIS).	☑	☐	
2.2.b	Are system configuration standards updated as new vulnerability issues are identified, as defined in Requirement 6.1?	☑	☐	
2.2.c	Are system configuration standards applied when new systems are configured?	☑	☐	
2.2.d	Do 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?	☑	☐	
2.2.1.a	Is only one primary function 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.	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
2.2.1.b	If virtualization technologies are used, is only one primary function implemented per virtual system component or device?	☑	☐	
2.2.2.a	Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?	☑	☐	
2.2.2.b	Are all enabled insecure services, daemons, or protocols justified per documented configuration standards?	☑	☐	
2.2.3	Are additional security features documented and implemented for any required services, protocols or daemons that are considered to be insecure?	☑	☐	
2.2.4.a	Are system administrators and/or personnel that configure system components knowledgeable about common security parameter settings for those system components?	☑	☐	
2.2.4.b	Are common system security parameters settings included in the system configuration standards?	☑	☐	
2.2.4.c	Are security parameter settings set appropriately on system components?	☑	☐	
2.2.5.a	Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	☑	☐	
2.2.5.b	Are enabled functions documented and do they support secure configuration?	☑	☐	
2.2.5.c	Is only documented functionality present on system components?	☑	☐	
2.3	Is non-console administrative access encrypted as follows:			
2.3.a	Is all non-console administrative access encrypted with strong cryptography, and is a strong encryption method invoked before the administrator's password is requested?	☑	☐	
2.3.b	Are system services and parameter files configured to prevent the use of Telnet and other insecure remote login commands?	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
2.3.c	Is administrator access to web-based management interfaces encrypted with strong cryptography?	☑	☐	
2.3.d	For the technology in use, is strong cryptography implemented according to industry best practice and/or vendor recommendations?	☑	☐	
2.4.a	Is an inventory maintained for systems components that are in scope for PCI DSS, including a list of hardware and software components and a description of function/use for each?	☑	☐	
2.4.b	Is the documented inventory kept current?	☑	☐	
2.5	Are security policies and operational procedures for managing vendor defaults and other security parameters: * Documented * In use * Known to all affected parties?	☑	☐	

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

PCI DSS Question		Response		
		Yes	No	N/A
3.1	Are data-retention and disposal policies, procedures, and processes implemented as follows:			
3.1.a	Is data storage amount and retention time limited to that required for legal, regulatory, and business requirements?	☑	☐	
3.1.b	Are there defined processes in place for securely deleting cardholder data when no longer needed for legal, regulatory, or business reasons?	☑	☐	
3.1.c	Are there specific retention requirements for cardholder data? For example, cardholder data needs to be held for X period for Y business reasons.	☑	☐	

PCI DSS Question		Response		
		Yes	No	N/A
3.1.d	Is there a quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements?	☑	☐	
3.1.e	Does all stored cardholder data meet the requirements defined in the data-retention policy?	☑	☐	
3.2.c	Is sensitive authentication data deleted or rendered unrecoverable upon completion of the authorization process?	☑	☐	
3.2.d	Do all systems adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):			
3.2.1	The full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored after authorization? This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: * The cardholder's name, * Primary account number (PAN), * Expiration date, and * Service code To minimize risk, store only these data elements as needed for business.	☑	☐	
3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored after authorization?	☑	☐	
3.2.3	The personal identification number (PIN) or the encrypted PIN block is not stored after authorization?	☑	☐	
3.3	Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN? Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.	☑	☐	

	PCI DSS Question	Response		
		Yes	No	N/A
3.4	Is PAN rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit logs), by using any of the following approaches? * One-way hashes based on strong cryptography (hash must be of the entire PAN) * Truncation (hashing cannot be used to replace the truncated segment of PAN) * Index tokens and pads (pads must be securely stored) * Strong cryptography with associated key management processes and procedures. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN	☑	☐	
3.4.1	If disk encryption (rather than file- or column-level database encryption) is used, is access managed as follows: Note: This requirement applies in addition to all other PCI DSS encryption and key management requirements.			
3.4.1.a	Is logical access to encrypted file systems managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials)?	☑	☐	
3.4.1.b	Are cryptographic keys stored securely (for example, stored on removable media that is adequately protected with strong access controls)?	☑	☐	
3.4.1.c	Is cardholder data on removable media encrypted wherever stored? Note: If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.	☑	☐	