Subpart D. This guidance applies to only the systems that are in scope for PCI, as defined by the PCI Security Standards Council.

Subpart B. Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters.

Item	*PCI DSS Requirement*	*Requirement Description*	*Applicable SAQ*			
			A	*B*	*C*	*D*
1	2.1	Change vendor-supplied security defaults before installing the system or device onto the network.			X	X
2	2.2	Develop configuration standards for all system components, based on industry-accepted system hardening standards. Configuration standards must include:				X
2a	2.2.1	Only one primary function per server.				X

Subpart H. Assign a Unique ID to Each Person with Computer Access.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	8.1, 8.2, 8.5.8	All users must have a unique ID which is, at a minimum, password protected.				X
2	8.5	User IDs must be securely issued and handled:				X
2a	8.5.1, 12.3.1	Authorization forms defining required access must be completed, approved by management, and filed				X
2b	8.5.2, 12.3.2	User identity must be verified prior to password resets				X
2c	8.5.3	First time passwords are unique, and must change immediately after the first use				X
2d	8.5.4	Terminated users have access revoked immediately				X
2e	8.5.5	Inactive accounts are disabled at least every 90 days				X
2f	8.5.6	Vendor maintenance accounts are enabled only during the time period needed, and immediately deactivated after use			X	X
2g	8.5.9	User passwords are changed at least every 90 days				X
2h	8.5.10, 8.5.11	Passwords				

Subpart I. Restrict Physical Access to Cardholder Data.

Item	PCI DSS Requirement	Requirement Description	

Subpart J. Track and Monitor All Access to Network Resources and Cardholder Data.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	10.1	Audit trails must link access to system components to an individual. Audit trails must include logging of:				X

Subpart K. Regularly Test Security System and Processes.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	11.1	Test for presence of wireless access points at least quarterly, or deploy wireless intrusion detection or intrusion prevention systems			X	X
2	11.2	Run internal vulnerability scans at least quarterly, and after significant changes			X	X
3	11.2	Have an external vulnerability scan conducted by a PCI Approved Scanning Vendor (ASV) at least quarterly			X	X
4	11.3(a)	Have an annual internal and external				

Subpart L. Maintain an Information Security Policy.

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
1	12.1.2, 12.1.3	Conduct an annual formal risk assessment that identifies threats and vulnerabilities, and update as the environment changes				X

Item	PCI DSS Requirement	Requirement Description	Applicable SAQ A	B	C	D
8e	12.9.1	Reference or include incident response procedures from the payment brands				X
8f	12.9.2	Test the plan at least annually				X
8g	12.9.3	Designate specific personnel to be available 24x7 to respond to alerts				X
8h	12.9.4	Provide appropriate incident response training to staff				X
8i	12.9.5	Include alerts from intrusion detection system / intrusion protection system (IDS, IPS) and file-integrity monitoring systems				X

[redacted]

and because it has various sensitivity classifications defined by federal law and state statute, it must be protected.

Subpart G. Demilitarized Zone (DMZ). Networks containing filtered anonymous or authenticated Internet accessible access devices or servers. Examples may include but are not limited to web email servers, instant messaging servers, virtual private network (VPN) or remote access servers/services, etc.

Subpart H. Electronic Cardholder Data. Data that must be protected by the PCI DSS defined as either all of the information found on the full magnetic strip, or the PAN plus any of the following: cardholder name, expiration data, service code.

Subpart I. Employee. Full-time and/or part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site.

Subpart J. May. A statement that is optional.

Subpart K. Merchant Bank. The merchant bank is a financial institution which offers financial services to organizations and individuals. The requirement to be PCI compliant is typically found in the contracts between merchant banks and entities with credit card processing accounts (a.k.a. merchant accounts).

Subpart L. Must. A statement that is required for a compliant implementation.

Subpart M. Must Not. A statement that is prohibited for a compliant implementation.

Subpart N. Payment Application Data Security Standard (PA DSS). Provides the definitive data standard for software vendors that develop payment applications.

Subpart O. Primary Account Number (PAN). Payment card number that identifies the issuer and the particular cardholder account.

Subpart P. Payment Card Industry Data Security Standards (PCI DSS). A standard that defines controls that must be in place around cardholder data. A contractual agreement with the merchant bank requires that all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands comply with this standard.

Subpart Q. Payment Brand. One of the brands of credit cards (e.g. MasterCard, Visa, American Express, etc).

Subpart R. Payment Cards. Cards containing payment data, used in purchasing goods and services. Typically referred to as either credit cards or debit cards.

Subpart S. PCI Data. Payment card information, as defined by the Payment Card Industry Security Standards Council. PCI data is subject to the PCI Data Security Standards. Such information includes payment account numbers (PANs) plus expiration dates, cardholder names, or verification codes, or data stored on track 2 of the payment card.

Subpart T. PCI Security Standards Council. The organization responsible for assembling, updating, and maintaining the PCI-DSS.

Subpart U. POS System. Point-of-Sale system.

Subpart V. Self Assessment Questionnaire. Merchants that process fewer than a given amount