Payment Card Industry (PCI)
Data Security Standard
Navigating PCI DSS

Understanding the Intent of the Requirements

Version 1.2

October 2008

Document Changes

Date	Version	Description
October 1, 2008	*1.2*	*To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.*

Table of Contents

Preface

This document describes the 12 Payment Card Industry Data Security Standard (PCI DSS) requirements, along with guidance to explain the intent of each requirement. This document is intended to assist merchants, service providers, and financial institutions who may want a clearer understanding of the Payment Card Industry Data Security Standard, and the specific meaning and intention behind the detailed requirements to secure system components (servers, network, applications etc) that support cardholder data environments.

NOTE: *Navigating PCI DSS: Understanding the Intent of the Requirements* is for guidance only. When completing a PCI DSS on-site assessment or Self Assessment Questionnaire (SAQ), the *PCI DSS Requirements and Security Assessment Procedures* and the *PCI DSS Self-Assessment Questionnaires v1.2* are the documents of record.

PCI DSS requirements apply to all system components that are included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data, including network components, servers and applications.

- Network components may include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types may include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
- Applications may include but not limited to all purchased and custom applications, including internal and external (Internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment. A Qualified Security Assessor (QSA) can assist in determining scope within an entity's cardholder data environment along with providing guidance about how to narrow the scope of a PCI DSS assessment by implementing proper network segmentation. For questions that pertain to whether a specific implementation is consistent with the standard or is 'compliant' with a specific requirement, PCI SSC recommends companies consult a Qualified Security Assessor (QSA) to validate their implementation of technology and processes, and compliance with the PCI Data Security Standard. QSAs' expertise in working with complex network environments lends well to providing best practices and guidance to the merchant or service provider attempting to achieve compliance. The PCI SSC List of Qualified Security Assessors can be found at: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Cardholder Data and Sensitive Authentication Data Elements

The following table illustrates commonly used elements of cardholder data and sensitive authentication data, whether **storage** of that data is permitted or prohibited, and whether each data element must be **protected**. This table is not meant to be exhaustive; its sole purpose is to illustrate the different type of requirements that apply to each data element.

Cardholder data is defined as the primary account number ("PAN," or credit card number) and other data obtained as part of a payment transaction, including the following data elements (see more detail below in the table):

- PAN
- Cardholder Name
- Expiration Date
- Service Code
- Sensitive Authentication Data: (1) full magnetic stripe data, (2) CAV2/CVC2/CVV2/CID, and (3) PINs/PIN blocks)

The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS. If PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply.

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3, 4
Cardholder Data	Primary Account Number	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

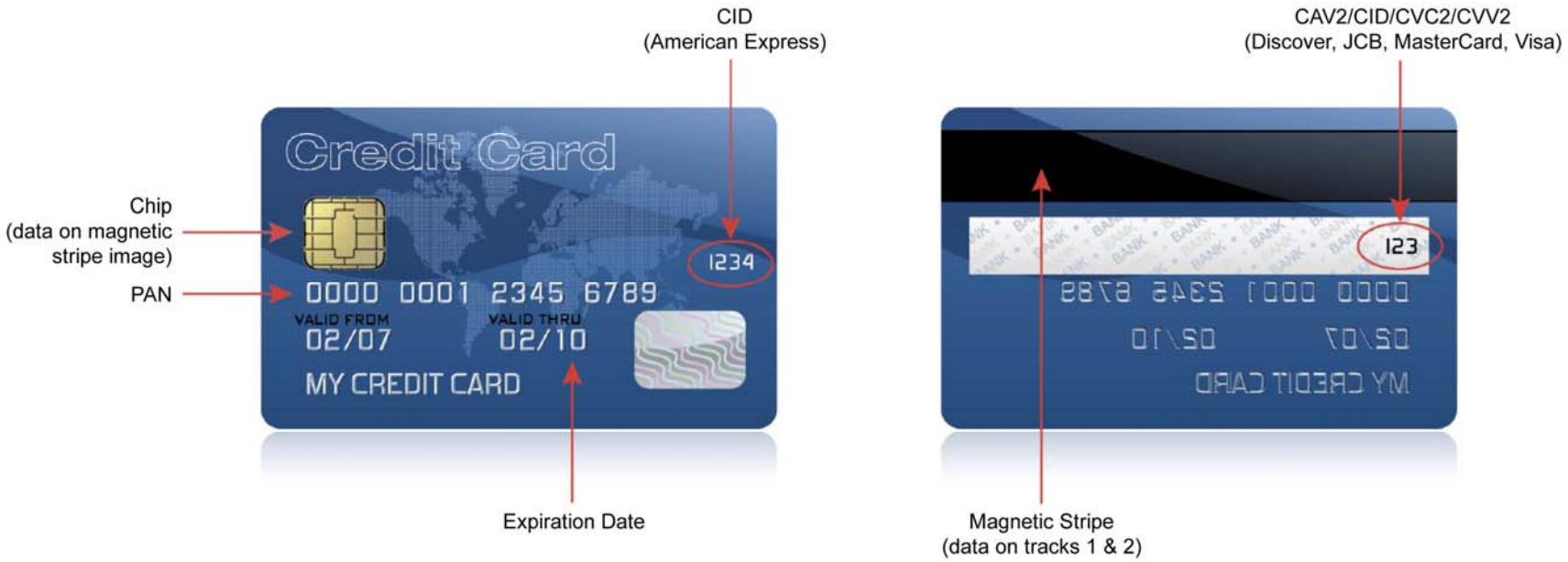
1 These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.

2 Sensitive authentication data must not be stored after authorization (even if encrypted).

3 Full track data from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.

Location of Cardholder Data and Sensitive Authentication Data

Sensitive authentication data consists of magnetic stripe (or track) data[4], card validation code or value[5], and PIN data[6]. **Storage of sensitive authentication data is prohibited!** This data is very valuable to malicious individuals as it allows them to generate fake payment cards and create fraudulent transactions. See *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for the full definition of "sensitive authentication data." The pictures of the back and front of a credit card below show the location of cardholder data and sensitive authentication data.



[4] Data encoded in the magnetic stripe used for authorization during a card-present transaction. This data may also be found in the magnetic stripe image on the chip, or elsewhere on the card. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are the primary account number, cardholder name, expiration date, and service code.

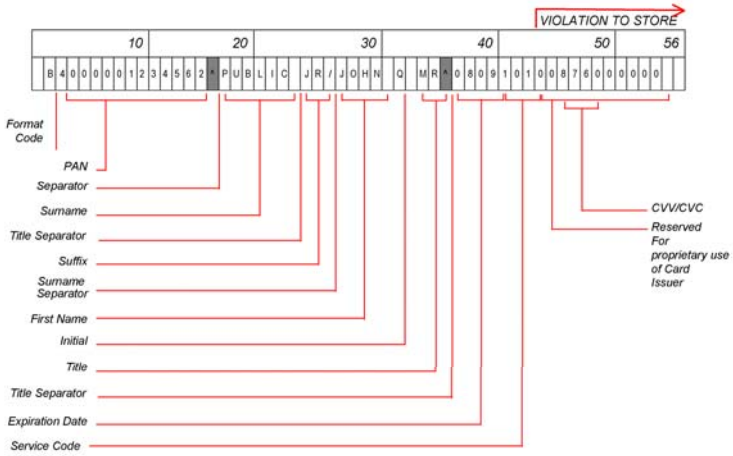
[5] The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

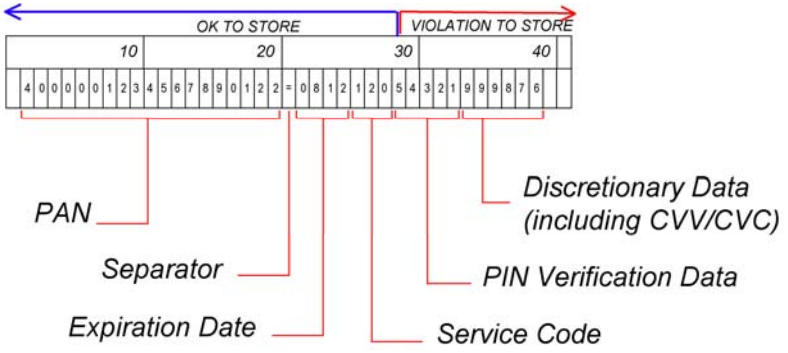
[6] Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Track 1 vs. Track 2 Data

If full track (either Track 1 or Track 2, from the magnetic stripe, magnetic-stripe image in a chip, or elsewhere) data is stored, malicious individuals who obtain that data can reproduce and sell payment cards around the world. Full track data storage also violates the payment brands' operating regulations and can lead to fines and penalties. The below illustration provides information about Track 1 and Track 2 data, describing the differences and showing the layout of the data as stored in the magnetic stripe.

Track 1	Track 2
▪ Contains all fields of both track 1 and track 2 ▪ Length up to 79 characters	▪ Shorter processing time for older dial-up transmissions ▪ Length up to 40 characters





Related Guidance for the PCI Data Security Standard

Build and Maintain a Secure Network

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

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Guidance for Requirements 1 and 2: Build and Maintain a Secure Network

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

Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the internet as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access, dedicated connection such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Requirement		Guidance
1.1	Establish firewall and router configuration standards that include the following:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Without policies and procedures in place to document how staff should configure firewalls and routers, a business could easily lose its first line of defense in data-protection. The policies and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.
1.1.1	A formal process for approving and testing all external network connections and changes to the firewall and router configurations	A policy and process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall.
1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	Network diagrams enable the organization to identify the location of all its network devices. Additionally, the network diagram can be used to map the data flow of cardholder data across the network and between individual devices in order to fully understand the scope of the cardholder data environment. Without current network and data flow diagrams, devices with cardholder data may be overlooked and may unknowingly be left out of the layered security controls implemented for PCI DSS and thus vulnerable to compromise.

Requirement		Guidance
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Using a firewall on every connection coming into (and out of) the network allows the organization to monitor and control access in and out, and to minimize the chances of a malicious individual's obtaining access to the internal network.
1.1.4	Description of groups, roles, and responsibilities for logical management of network components	This description of roles and assignment of responsibility ensures that someone is clearly responsible for the security of all components and is aware of their responsibility, and that no devices are left unmanaged.
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities—and many organizations are vulnerable to these types of compromises because they do not patch security vulnerabilities for services, protocols, and ports they don't use (even though the vulnerabilities are still present). Each organization should clearly decide which services, protocols, and ports are necessary for their business, document them for their records, and ensure that all other services, protocols, and ports and disabled or removed. Also, organizations should consider blocking all traffic and only re-opening those ports once a need has been determined and documented. Additionally, there are many services, protocols, or ports that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. If these insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed.
1.1.6	Requirement to review firewall and router rule sets at least every six months	This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match business justifications. It is advisable to undertake these reviews on a more frequent basis, such as monthly, to ensure that the rule sets are current and match the needs of the business without opening security holes and running unnecessary risks.

Requirement	Guidance
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment. *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.*	It is essential to install network protection, namely a firewall, between the internal, trusted network and any other untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly means that the entity will be vulnerable to unauthorized access by malicious individuals or software. If a firewall is installed but does not have rules that control or limit certain traffic, malicious individuals may still be able to exploit vulnerable protocols and ports to attack your network.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment	This requirement is intended to prevent malicious individuals from accessing the organization's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an untrusted server. All firewalls should include a rule that denies all inbound and outbound traffic not specifically needed. This will prevent inadvertent holes that would allow other, unintended and potentially harmful traffic in or out.
1.2.2 Secure and synchronize router configuration files.	While running configuration files are usually implemented with secure settings, the start-up files (routers only run these files upon re-start) may not be implemented with the same secure settings because they only run occasionally. When a router does re-start without the same secure settings as those in the running configuration files, it may result in weaker rules that allow malicious individuals into the network, because the start-up files may not be implemented with the same secure settings as the running configuration files.
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny any traffic from the wireless environment or to control any traffic (if such traffic is necessary for business purposes).	The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and cardholder data. If a wireless device or network is installed without a company's knowledge, a malicious individual could easily and "invisibly" enter the network. If firewalls do not restrict access from wireless networks into the payment card environment, malicious individuals that gain unauthorized access to the wireless network can easily connect to the payment card environment and compromise account information.

Requirement	Guidance
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	A firewall's intent is to manage and control all connections between public systems and internal systems (especially those that store cardholder data). If direct access is allowed between public systems and those that store cardholder data, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.
1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	These requirements are intended to prevent malicious individuals from accessing the organization's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an external untrusted server in an untrusted network).
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	
1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	The DMZ is the part of the firewall that faces the public Internet and manages connections between the Internet and internal services that an organization needs to have available to the public (like a web server). It is the first line of defense in isolating and separating traffic that needs to communicate with the internal network from traffic that does not.
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ**.**	Normally a packet contains the IP address of the computer that originally sent it. This allows other computers in the network to know where it came from. In certain cases, this sending IP address will be spoofed by malicious individuals. For example, malicious individuals send a packet with a spoofed address, so that (unless your firewall prohibits it) the packet will be able to come into your network from the Internet, looking like it is internal, and therefore legitimate, traffic. Once the malicious individual is inside your network, they can begin to compromise your systems. Ingress filtering is a technique you can use on your firewall to filter packets coming into your network to, among other things, ensure packets are not “spoofed” to look like they are coming from your own internal network. For more information on packet filtering, consider obtaining information on a corollary technique called “egress filtering.”
1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	The DMZ also should evaluate all traffic outbound from inside the network to ensure that all outbound traffic follows established rules. For the DMZ to serve this function effectively, connections from inside the network to any addresses outside the network should not be allowed unless they first go through and are evaluated for legitimacy by the DMZ.

Requirement	Guidance
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.)	A firewall that performs stateful packet inspection keeps "state" (or the status) for each connection to the firewall. By keeping "state," the firewall knows whether what appears to be a response to a previous connection is truly a response (since it "remembers" the previous connection) or is a malicious individual or software trying to spoof or trick the firewall into allowing the connection.
1.3.7 Place the database in an internal network zone, segregated from the DMZ.	Cardholder data requires the highest level of information protection. If cardholder data is located within the DMZ, access to this information is easier for an external attacker, since there are fewer layers to penetrate.
1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).	IP masquerading, which is managed by the firewall, allows an organization to have internal addresses that are only visible inside the network and external address that are visible externally. If a firewall does not “hide” or mask the IP addresses of the internal network, a malicious individual could discover internal IP addresses and attempt to access the network with a spoofed IP address.
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.	If a computer does not have a firewall or anti-virus program installed, spyware, Trojans, viruses, worms and rootkits (malware) may be downloaded and/or installed unknowingly. The computer is even more vulnerable when directly connected to the Internet and not behind the corporate firewall. Malware loaded on a computer when not behind the corporate firewall can then maliciously target information within the network when the computer is re-connected to the corporate network.

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

Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

Requirement		Guidance
2.1	Always change vendor-supplied defaults **before** installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	Malicious individuals (external and internal to a company) often use vendor default settings, account names, and passwords to compromise systems. These settings are well known in hacker communities and leave your system highly vulnerable to attack.
2.1.1	**For wireless environments** connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	Many users install these devices without management approval and do not change default settings or configure security settings. If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack your network. In addition, the key exchange protocol for the older version of 802.11x encryption (WEP) has been broken and can render the encryption useless. Verify that firmware for devices are updated to support more secure protocols like WPA/WPA2.
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, security organizations have established system-hardening recommendations, which advise how to correct these weaknesses. If systems are left with these weaknesses—for example, weak file settings or default services and protocols (for services or protocols that are often not needed)—an attacker will be able to use multiple, known exploits to attack vulnerable services and protocols, and thereby gain access to your organization's network. Visit these three examples of websites where you can learn more about industry best practices that can help you implement configuration standards: www.nist.gov, www.sans.org, www.cisecurity.org.

Requirement	Guidance
2.2.1 Implement only one primary function per server.	This is intended to ensure your organization's system configuration standards and related processes address server functions that need to have different security levels, or that may introduce security weaknesses to other functions on the same server. For example: 1. A database, which needs to have strong security measures in place, would be at risk sharing a server with a web application, which needs to be open and directly face the Internet. 2. Failure to apply a patch to a seemingly minor function could result in a compromise that impacts other, more important functions (such as a database) on the same server. This requirement is meant for servers (usually Unix, Linux, or Windows based), but not mainframe systems.
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).	As stated at 1.1.7, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. To ensure that these services and protocols are always disabled when new servers are deployed, this requirement should be part of your organization's configuration standards and related processes.
2.2.3 Configure system security parameters to prevent misuse.	This is intended to ensure your organization's system configuration standards and related processes specifically address security settings and parameters that have known security implications.
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	The server-hardening standards must include processes to address unnecessary functionality with specific security implications (like removing/disabling FTP or the web server if the server will not be performing those functions).
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	If remote administration is not done with secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data.

Requirement		Guidance
2.4	Shared hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in *"Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers*."	This is intended for hosting providers that provide shared hosting environments for multiple clients on the same server. When all data is on the same server and under control of a single environment, often the settings on these shared servers are not manageable by individual clients, allow clients to add insecure functions and scripts that impact the security of all other client environments; and thereby make it easy for a malicious individual to compromise one client's data and thereby gain access to all other clients' data. See Appendix A

Guidance for Requirements 3 and 4: Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Protection measures such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for definitions of "strong cryptography" and other PCI DSS terms.*

Requirement		Guidance
3.1	Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	Extended storage of cardholder data that exceeds business need creates an unnecessary risk. The only cardholder data that may be stored is the primary account number or PAN (rendered unreadable), expiration date, name, and service code. **Remember, if you don't need it, don't store it!**
3.2	Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements, 3.2.1 through 3.2.3*:*	Sensitive authentication data consists of magnetic stripe (or track) data[7], card validation code or value[8], and PIN data[9]. **Storage of sensitive authentication data after authorization is prohibited!** This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. See *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for the full definition of "sensitive authentication data."

[7] Data encoded in the magnetic stripe used for authorization during a card-present transaction. This data may also be found in the magnetic stripe image on the chip, or elsewhere on the card. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are the primary account number, cardholder name, expiration date, and service code.

[8] The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

[9] Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Requirement		Guidance
3.2.1	Do not store the full contents of any track from the magnetic stripe (located is on the back of a card, contained in a chip, or elsewhere). 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.* *Note: See* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.*	If full track data is stored, malicious individuals who obtain that data can reproduce and sell payment cards around the world.
3.2.2	Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions *Note: See* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.*	The purpose of the card validation code is to protect "card-not-present" transactions—Internet or mail order/telephone order (MO/TO) transactions—where the consumer and the card are not present. These types of transactions can be authenticated as coming from the card owner only by requesting this card validation code, since the card owner has the card in-hand and can read the value. If this prohibited data is stored and subsequently stolen, malicious individuals can execute fraudulent Internet and MO/TO transactions.
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	These values should be known only to the card owner or bank that issued the card. If this prohibited data is stored and subsequently stolen, malicious individuals can execute fraudulent PIN-based debit transactions (for example, ATM withdrawals).

Requirement		Guidance
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Notes:* ▪ *This requirement does not apply to employees and other parties with a specific need to see the full PAN;* ▪ *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point of sale [POS] receipts.*	The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. The PAN can be displayed in full form on the "merchant copy" receipts; however the paper receipts should adhere to the same security requirements as electronic copies and follow the guidelines of the PCI Data Security Standard, especially Requirement 9 regarding physical security. The full PAN can also be displayed for those with a legitimate business need to see the full PAN.
3.4	Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs) by using any of the following approaches:	Lack of protection of PANs can allow malicious individuals to view or download this data. PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. Damage from theft or loss of backup tapes during transport can be reduced by ensuring PANs are rendered unreadable via encryption, truncation, or hashing. Since audit, troubleshooting, and exception logs have to be retained, you can prevent disclosure of data in logs by rendering PANs unreadable (or removing or masking them) in logs. Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography"
	▪ One-way hashes based on strong cryptography	One-way hash functions (such as SHA-1) based on strong cryptography can be used to render cardholder data unreadable. Hash functions are appropriate when there is no need to retrieve the original number (one-way hashes are irreversible).
	▪ Truncation	The intent of truncation is that only a portion (not to exceed the first six and last four digits) of the PAN is stored. This is different from masking, where the whole PAN is stored but the PAN is masked when displayed (i.e., only part of the PAN is displayed on screens, reports, receipts, etc.).
	▪ Index tokens and pads (pads must be securely stored)	Index tokens and pads may also be used to render cardholder data unreadable. An index token is a cryptographic token that replaces the PAN based on a given index for an unpredictable value. A one-time pad is a system in which a private key, generated randomly, is used only once to encrypt a message that is then decrypted using a matching one-time pad and key.

Requirement	Guidance
▪ Strong cryptography with associated key-management processes and procedures. *The MINIMUM account information that must be rendered unreadable is the PAN.* *Notes:* ▪ *If for some reason, a company is unable to render the PAN unreadable, refer to "Appendix B: Compensating Controls."* ▪ *"Strong cryptography" is defined in* the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*.*	The intent of strong cryptography (see definition and key lengths in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*) is that the encryption be based on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm).
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	The intent of this requirement is to address the acceptability of disk encryption for rendering cardholder data unreadable. Disk encryption encrypts data stored on a computer's mass storage and automatically decrypts the information when an authorized user requests it. Disk encryption systems intercept operating system read and write operations and carry out the appropriate cryptographic transformations without any special action by the user other than supplying a password or pass phrase at the beginning of a session. Based on these characteristics of disk encryption, to be compliant with this requirement, the disk encryption method cannot have: 1) A direct association with the operating system, or 2) Decryption keys that are associated with user accounts.
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:	Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data.
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary	There should be very few who have access to cryptographic keys, usually only those who have key custodian responsibilities.
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	Cryptographic keys must be stored securely, usually encrypted with key-encrypting keys, and stored in very few locations.

Requirement		Guidance
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	The manner in which cryptographic keys are managed is a critical part of the continued security of the encryption solution. A good key management process, whether it is manual or automated as part of the encryption product, addresses all key elements at 3.6.1 through 3.6.8.
3.6.1	Generation of strong cryptographic keys	The encryption solution must generate strong keys, as defined in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* under "strong cryptography."
3.6.2	Secure cryptographic key distribution	The encryption solution must distribute keys securely, meaning the keys are not distributed in the clear, and only to custodians identified in 3.5.1.
3.6.3	Secure cryptographic key storage	The encryption solution must store keys securely, meaning the keys are not stored in the clear (encrypt them with a key-encryption key).
3.6.4	Periodic cryptographic key changes • As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically • At least annually	If provided by encryption application vendor, follow any vendor processes or recommendations for periodic changing of keys. Annual changing of encryption keys is imperative to minimize the risk of someone's obtaining the encryption keys, and being able to decrypt data.
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys	Old keys that are no longer used or needed should be retired and destroyed to ensure that the keys can no longer be used. If old keys need to be kept (to support archived, encrypted data, for example) they should be strongly protected. (See 3.6.6 below.) The encryption solution should also allow for and facilitate a process to replace keys that are known to be, or suspected of being, compromised.
3.6.6	Split knowledge and establishment of dual control of cryptographic keys	Split knowledge and dual control of keys are used to eliminate the possibility of one person's having access to the whole key. This control is usually applicable for manual key-encryption systems, or where key management is not implemented by the encryption product. This type of control is usually implemented within hardware security modules.
3.6.7	Prevention of unauthorized substitution of cryptographic keys	The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.

Requirement		Guidance
3.6.8	Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.	This process will ensure the individual commits to the key-custodian role and understands his/her responsibilities.

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

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Requirement		Guidance
4.1	Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are:* ▪ *The Internet,* ▪ *Wireless technologies,* ▪ *Global System for Mobile Communications (GSM), and* ▪ *General Packet Radio Service (GPRS.*	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. Secure Sockets Layer encrypts web pages and the data entered into them. When using SSL secured websites, ensure "https" is part of the URL. Note that SSL versions prior to v3.0 contain documented vulnerabilities, such as buffer overflows, that an attacker can use to gain control of the affected system.
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ▪ *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* ▪ *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*	Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of appropriate encryption can prevent eavesdropping and disclosure of sensitive information across the network. Many known compromises of cardholder data stored only in the wired network originated when a malicious user expanded access from an insecure wireless network. Strong encryption for authentication and transmission of cardholder data is required to prevent malicious users from gaining access to the wireless network— the data on the network—or utilizing the wireless networks to get to other internal networks or data. WEP does not utilize strong encryption. WEP encryption should never be used alone since it is vulnerable due to weak initial vectors (IV) in the WEP key-exchange process, and lack of required rotation of keys. An attacker can use freely available brute-force cracking tools to penetrate WEP encryption. Current wireless devices should be upgraded (example: upgrade access point firmware to WPA) to support strong encryption. If current devices cannot be upgraded, new equipment should be purchased. If wireless networks are utilizing WEP, they should not have access to cardholder data environments.

Requirement		Guidance
4.2	Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).	E-mail, instant messaging, and chat can be easily intercepted by packet-sniffing during delivery traversal across internal and public networks. Do not utilize these messaging tools to send PAN unless they can provide encryption capabilities.

Guidance for Requirements 5 and 6: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

Requirement		Guidance
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	There is a constant stream of attacks using widely published exploits, often "0 day" (published and spread throughout networks within an hour of discovery) against otherwise secured systems. Without anti-virus software that is updated regularly, these new forms of malicious software can attack and disable your network. Malicious software may be unknowingly downloaded and/or installed from the internet, but computers are also vulnerable when using removable storage devices such as CDs and DVDs, USB memory sticks and hard drives, digital cameras, personal digital assistants (PDAs) and other peripheral devices. Without anti-virus software installed, these computers may become access points into your network, and/or maliciously target information within the network. While systems that are commonly affected by malicious software typically do not include mainframes and most Unix systems (see more detail below), each entity must have a process according to PCI DSS Requirement 6.2 to identify and address new security vulnerabilities and update their configuration standards and processes accordingly. Trends in malicious software related to operating systems an entity uses should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into the company's configuration standards and protection mechanisms as needed. Typically, the following operating systems are not commonly affected by malicious software: mainframes, and certain Unix servers (such as AIX, Solaris, and HP-Unix). However, industry trends for malicious software can change quickly and each organization must comply with Requirement 6.2 to identify and address new security vulnerabilities and update their configuration standards and processes accordingly.

Requirement		Guidance
5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	It is important to protect against **ALL** types and forms of malicious software.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	The best anti-virus software is limited in effectiveness if it does not have current anti-virus signatures or if it isn't active in the network or on an individual's computer. Audit logs provide the ability to monitor virus activity and anti-virus reactions.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

Requirement		Guidance
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	There are a considerable amount of attacks using widely published exploits, often "0 day" (published within the hour) against otherwise secured systems. Without implementing the most recent patches on critical systems as soon as possible, a malicious individual can use these exploits to attack and disable the network. Consider prioritizing changes such that critical security patches on critical or at-risk systems can be installed within 30 days, and other less-risky changes are installed within 2-3 months.
6.2	Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.	The intention of this requirement is that organizations are kept up-to-date with new vulnerabilities so they can appropriately protect their network, and incorporate newly discovered and relevant vulnerabilities into their configuration standards.
6.3	Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices and incorporate information security throughout the software development life cycle. These processes must include the following:	Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment.

Requirement	Guidance
6.3.1 Testing of all security patches, and system and software configuration changes before deployment **6.3.1.1** Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.) **6.3.1.2** Validation of proper error handling **6.3.1.3** Validation of secure cryptographic storage **6.3.1.4** Validation of secure communications **6.3.1.5** Validation of proper role-based access control (RBAC)	Ensure all installations and changes are performing as expected, and that they do not have any functions that are unexpected, unwanted, or harmful.
6.3.2 Separate development/test and production environments	Often development and test environments are less secure than the production environment. Without adequate separation, the production environment and cardholder data may be at risk due to vulnerabilities or weak internal processes.
6.3.3 Separation of duties between development/test and production environments	This minimizes the number of personnel with access to the production environment and cardholder data, and helps ensure that access is limited to those who truly need that access.
6.3.4 Production data (live PANs) are not used for testing or development	Security controls are usually not as stringent in the development environment. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).
6.3.5 Removal of test data and accounts before production systems become active	Test data and accounts should be removed from production code before the application becomes active, since these items may give away information about the functioning of the application. Possession of such information could facilitate compromise of the application and related cardholder data.
6.3.6 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers	Custom application accounts, user IDs, and passwords should be removed from production code before the application becomes active or are released to customers, since these items may give away information about the functioning of the application. Possession of such information could facilitate compromise of the application and related cardholder data.

Requirement		Guidance
6.3.7	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	Security vulnerabilities in custom code are commonly exploited by malicious individuals to gain access to a network and compromise cardholder data. Those with knowledge of secure coding techniques should review code to identify vulnerabilities.
6.4	Follow change control procedures for all changes to system components. The procedures must include the following:	Without proper software change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced. If related personnel policies for background checks and system access controls are not adequate, there is a risk that untrustworthy and untrained individuals may have unrestricted access to software code, terminated employees may have the opportunity to compromise systems, and unauthorized actions may not be detected.
6.4.1	Documentation of impact	The impact of the change should be documented so that all affected parties will be able to plan appropriately for any processing changes.
6.4.2	Management sign-off by appropriate parties	Management approval indicates that the change is a legitimate and authorized change sanctioned by the organization.
6.4.3	Testing of operational functionality	Thorough testing should be performed to verify that all actions are expected, reports are accurate, that all possible error conditions react properly, etc.
6.4.4	Back-out procedures	For each change, there should be back-out procedures in case the change fails, to allow for restoring back to the previous state.

Requirement	Guidance
6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the *Open Web Application Security Project Guide.* Cover prevention of common coding vulnerabilities in software development processes, to include the following: *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.*	The application layer is high-risk and may be targeted by both internal and external threats. Without proper security, cardholder data and other confidential company information can be exposed, resulting in harm to a company, its customers, and its reputation.
6.5.1 Cross-site scripting (XSS)	All parameters should be validated before inclusion. XSS flaws occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc.
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.	Validate input to verify user data cannot modify meaning of commands and queries. Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data, and allows the attacker to attack components inside the network through the application, to initiate attacks such as buffer overflows, or to reveal both confidential information and server application functionality. This is also a popular way to conduct fraudulent transactions on commerce-enabled web sites. Information from web requests should be validated before being sent to the web application - for example, by checking for all alpha characters, mix of alpha and numeric characters, etc.
6.5.3 Malicious file execution	Validate input to verify application does not accept unexpected filenames or files from users. Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.

Requirement		Guidance
6.5.4	Insecure direct object references	Do not expose internal object references to users. A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.
6.5.5	Cross-site request forgery (CSRF)	Do not reply on authorization credentials and tokens automatically submitted by browsers. A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.
6.5.6	Information leakage and improper error handling	Do not leak information via error messages or other means. Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks. Also, incorrect error handling provides information that helps a malicious individual compromise the system. If a malicious individual can create errors that the web application does not handle properly, they can gain detailed system information, create denial-of-service interruptions, cause security to fail, or crash the server. For example, the message "incorrect password provided" tells them the user ID provided was accurate and that they should focus their efforts only on the password. Use more generic error messages, like "data could not be verified."
6.5.7	Broken authentication and session management	Properly authenticate users and protect account credentials and session tokens. Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.
6.5.8	Insecure cryptographic storage	Prevent cryptographic flaws. Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.
6.5.9	Insecure communications	Properly encrypt all authenticated and sensitive communications. Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.

Requirement		Guidance
	6.5.10 Failure to restrict URL access	Consistently enforce access control in presentation layer and business logic for all URLs. Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: ▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ▪ Installing a web-application firewall in front of public-facing web applications	Attacks on web-facing applications are common and often successful, and are allowed by poor coding practices. This requirement for reviewing applications or installing web-application firewalls is intended to greatly reduce the number of compromises on public-facing web applications that result in breaches of cardholder data. ▪ Manual or automated vulnerability security assessment tools or methods that review and/or scan for application vulnerabilities can be used to satisfy this requirement ▪ Web-application firewalls filter and block non-essential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured. See *Information Supplement*: *Requirement 6.6 Application Reviews and Web-Application Firewalls Clarified* (www.pcisecuritystandards.org) for more information.

Guidance for Requirements 7, 8, and 9: Implement Strong Access Control Measures

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

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Requirement	Guidance
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: **7.1.1** Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities **7.1.2** Assignment of privileges is based on individual personnel's job classification and function **7.1.3** Requirement for an authorization form signed by management that specifies required privileges **7.1.4** Implementation of an automated access control system	The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a strong business reason for the access helps your organization prevent mishandling of cardholder data through inexperience or malice. When access rights are granted only to the least amount of data and privileges needed to perform a job, this is a called "need to know," and when privileges are assigned to individuals based on job classification and function, this is called "role-based access control" or RBAC. Your organization should create a clear policy and processes for data access control based on "need to know" and using "role-based access control," to define how, and to whom, access is granted.
7.2 Establish a mechanism for system components with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. This access control system must include the following: *Note: "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.* **7.2.1** Coverage of all system components **7.2.2** Assignment of privileges to individuals based on job classification and function **7.2.3** Default "deny-all" setting	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Use of an automated access control system or mechanism is essential to manage multiple users. This system should be established in accordance with your organization's access control policy and processes (including "need to know" and "role-based access control"), should manage access to all system components, and should have a default "deny-all" setting to ensure no one is granted access until and unless a rule is established specifically granting such access.

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Requirement		Guidance
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.
8.2	In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: ▪ Password or passphrase ▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	These authentication items, when used in addition to unique IDs, help protect users' unique IDs from being compromised (since the one attempting the compromise needs to know both the unique ID and the password or other authentication item).
8.3	Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	Two-factor authentication requires two forms of authentication for higher-risk accesses, such as those originating from outside your network. For additional security, your organization can also consider using two-factor authentication when accessing networks of higher security from networks of lower security—for example, from corporate desktops (lower security) to production servers/databases with cardholder data (high security).
8.4	Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*).	Many network devices and applications transmit the user ID and unencrypted password across the network and/or also store the passwords without encryption. A malicious individual can easily intercept the unencrypted or readable user ID and password during transmission using a "sniffer," or directly access the user IDs and unencrypted passwords in files where they are stored, and use this stolen data to gain unauthorized access.
8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for user authentication and password management.

Requirement		Guidance
8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	To ensure users added to your systems are all valid and recognized users, the addition, deletion, and modification of user IDs should be managed and controlled by a small group with specific authority. The ability to manage these user IDs should be limited to only this small group.
8.5.2	Verify user identity before performing password resets.	Many malicious individuals use "social engineering"—for example, calling a help desk and acting as a legitimate user—to have a password changed so they can utilize a user ID. Consider use of a "secret question" that only the proper user can answer to help administrators identify the user prior to re-setting passwords. Ensure such questions are secured properly and not shared.
8.5.3	Set first-time passwords to a unique value for each user and change immediately after the first use.	If the same password is used for every new user set up, an internal user, former employee, or malicious individual may know or easily discover this password, and use it to gain access to accounts.
8.5.4	Immediately revoke access for any terminated users.	If an employee has left the company, and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur. This access could happen from the former employee or from a malicious user who exploits the older and/or unused account. Consider implementing a process with HR for immediate notification when an employee is terminated so that the user account can be quickly deactivated.
8.5.5	Remove/disable inactive user accounts at least every 90 days.	Existence of inactive accounts allows an unauthorized user exploit the unused account to potentially access cardholder data.
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed.	Allowing vendors (like POS vendors) to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-ready external entry point into your network. Please also see 12.3.8 and 12.3.9 for more on this topic.
8.5.7	Communicate password procedures and policies to all users who have access to cardholder data.	Communicating password procedures to all users helps those users understand and abide by the policies, and to be alert for any malicious individuals who may attempt to exploit their passwords to gain access to cardholder data (for example, by calling an employee and asking for their password so the caller can "troubleshoot a problem").

Requirement		Guidance
8.5.8	Do not use group, shared, or generic accounts and passwords.	If multiple users share the same account and password, it becomes impossible to assign accountability for, or to have effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that shares the account and password.
8.5.9	Change user passwords at least every 90 days.	Strong passwords are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. There is more time for a malicious individual to find these weak accounts, and compromise a network under the guise of a valid user ID, if passwords are short, simple to guess, or valid for a long time without a change. Strong passwords can be enforced and maintained per these requirements by enabling the password and account security features that come with your operating system (for example, Windows), networks, databases and other platforms.
8.5.10	Require a minimum password length of at least seven characters.	
8.5.11	Use passwords containing both numeric and alphabetic characters.	
8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	
8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.
8.5.14	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of these locked accounts stops the malicious individual from continually guessing the password (they will have to stop for a minimum of 30 minutes until the account is reactivated). Additionally, if reactivation must be requested, the admin or help desk can validate that the account owner is the cause (from typing errors) of the lockout.
8.5.15	If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	When users walk away from an open machine with access to critical network or cardholder data, that machine may be used by others in the user's absence, resulting in unauthorized account access and/or account misuse.

Requirement		Guidance
8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	Without user authentication for access to databases and applications, the potential for unauthorized or malicious access increases, and such access cannot be logged since the user has not been authenticated and is therefore not known to the system. Also, database access should be granted through programmatic methods only (for example, through stored procedures), rather than via direct access to the database by end users (except for DBAs, who can have direct access to the database for their administrative duties).

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

Requirement			Guidance
9.1		Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Without physical access controls, unauthorized persons could potentially gain access to the building and to sensitive information, and could alter system configurations, introduce vulnerabilities into the network, or destroy or steal equipment.
	9.1.1	Use video cameras or other access control mechanisms to monitor individual access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.*	When investigating physical breaches, these controls can help identify individuals that physically access those areas storing cardholder data.
	9.1.2	Restrict physical access to publicly accessible network jacks	Restricting access to network jacks will prevent malicious individuals from plugging into readily available network jacks that may allow them access into internal network resources. Consider turning off network jacks while not in use, and reactivating them only while needed. In public areas such as conference rooms, establish private networks to allow vendors and visitors to access Internet only so that they are not on your internal network.
	9.1.3	Restrict physical access to wireless access points, gateways, and handheld devices.	Without security over access to wireless components and devices, malicious users could use your company's unattended wireless devices to access your network resources, or even connect their own devices to your wireless network, giving them unauthorized access. Consider placing wireless access points and gateways in secure storage areas, such as within locked closets or server rooms. Ensure strong encryption is enabled. Enable automatic device lockout on wireless handheld devices after a long idle period, and set your devices to require a password when powering on.

Requirement		Guidance
9.2	Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. *For purposes of this requirement, "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.*	Without badge systems and door controls, unauthorized and malicious users can easily gain access to your facility to steal, disable, disrupt, or destroy critical systems and cardholder data. For optimum control, consider implementing badge or card access system in and out of work areas that contain cardholder data.
9.3	Make sure all visitors are handled as follows:	Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to your facilities (and potentially, to cardholder data).
	9.3.1 Authorized before entering areas where cardholder data is processed or maintained. **9.3.2** Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees. **9.3.3** Asked to surrender the physical token before leaving the facility or at the date of expiration.	Visitor controls are important to ensure visitors only enter areas they are authorized to enter, that they are identifiable as visitors so employees can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.
9.4	Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	A visitor log documenting minimum information on the visitor is easy and inexpensive to maintain and will assist, during a potential data breach investigation, in identifying physical access to a building or room, and potential access to cardholder data. Consider implementing logs at the entry to facilities and especially into zones where cardholder data is present.
9.5	Store media backups in a secure location, preferably in an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	If stored in a non-secured facility, backups that contain cardholder data may easily be lost, stolen, or copied for malicious intent. For secure storage, consider contracting with a commercial data storage company OR, for a smaller entity, using a safe-deposit box at a bank.

Requirement			Guidance
9.6	Physically secure all paper and electronic media that contain cardholder data.		Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on portable media, printed out, or left on someone's desk. Consider procedures and processes for protecting cardholder data on media distributed to internal and/or external users. Without such procedures data can be lost or stolen and used for fraudulent purposes.
9.7	Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:		
	9.7.1	Classify the media so it can be identified as confidential.	Media not identified as confidential may not be treated with the care it requires and may be lost or stolen. Include a media classification process in the procedures recommended in Requirement 9.6 above.
	9.7.2	Send the media by secured courier or other delivery method that can be accurately tracked.	Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. Use the services of a secure courier to deliver any media that contains cardholder data, so that you can use their tracking systems to maintain inventory and location of shipments.
9.8	Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).		Cardholder data leaving secure areas without a process approved by management can lead to lost or stolen data. Without a firm process, media locations are not tracked, nor is there a process for where the data goes or how it is protected. Include development of a management-approved process for moving media in the procedures recommended in Requirement 9.6 above.
9.9	Maintain strict control over the storage and accessibility of media that contains cardholder data.		Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time. Include development of a process to limit access to media with cardholder data in the procedures recommended above in Requirement 9.6.
	9.9.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	If media is not inventoried, stolen or lost media may not be noticed for a long time. Include development of a process for media inventories and secure storage in the procedures recommended above in Requirement 9.6.

Requirement		Guidance
9.10	Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:	If steps are not taken to destroy information contained on PC hard disks and CDs, and on paper, disposal of such information may result in compromise and lead to financial or reputation loss. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trashcans and recycle bins, and use found information to launch an attack. Include development of a process for properly destroying media with cardholder data, including proper storage of such media prior to destruction, in the procedures recommended above in Requirement 9.6.
9.10.1	Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed	
9.10.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	

Guidance for Requirements 10 and 11: Regularly Monitor and Test Networks

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

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

Requirement	Guidance
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	It is critical to have a process or system that links user access to system components accessed, and in particular, for those users with administrative privileges. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user. Post-incident forensic teams heavily depend on these logs to initiate the investigation.
10.2 Implement automated audit trails for all system components to reconstruct the following events: **10.2.1** All individual user accesses to cardholder data **10.2.2** All actions taken by any individual with root or administrative privileges **10.2.3** Access to all audit trails **10.2.4** Invalid logical access attempts **10.2.5** Use of identification and authentication mechanisms **10.2.6** Initialization of the audit logs **10.2.7** Creation and deletion of system-level objects.	Malicious individuals on the network will often perform multiple access attempts on targeted systems. Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up.

Requirement	Guidance
10.3 Record at least the following audit trail entries for all system components for each event: **10.3.1** User identification **10.3.2** Type of event **10.3.3** Date and time **10.3.4** Success or failure indication **10.3.5** Origination of event **10.3.6** Identity or name of affected data, system component, or resource	By recording these entries for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, where, and how.
10.4 Synchronize all critical system clocks and times.	If a malicious individual has entered the network, they will often attempt to change the time stamps of their actions within the audit logs to prevent detection of their activity. For post-incident forensics teams, the time of each activity is critical in determining how the systems were compromised. A malicious individual may also try to directly change the clock on a time server, if access restrictions are not appropriate, to restate the time to before the malicious individual was in the network.
10.5 Secure audit trails so they cannot be altered.	Often a malicious individual who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.
10.5.1 Limit viewing of audit trails to those with a job-related need. **10.5.2** Protect audit trail files from unauthorized modifications. **10.5.3** Promptly back up audit trail files to a centralized log server or media that is difficult to alter. **10.5.4** Write logs for external-facing technologies onto a log server on the internal LAN.	Adequate protection of the audit logs includes strong access control (limit access to logs based on “need to know” only) and use of internal segregation (to make the logs harder to find and modify). By writing logs from external-facing technologies such as wireless, firewalls, DNS, and mail servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network.

Requirement		Guidance
10.5.5	Use file-integrity monitoring and change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	File-integrity monitoring systems check for changes to critical files, and notify when such changes are noted. For file-integrity monitoring purposes, an entity usually monitors files that don't regularly change, but when changed indicate a possible compromise. For log files (which do change frequently) what should be monitored are, for example, when a log file is deleted, suddenly grows or shrinks significantly, and any other indicators that a malicious individual has tampered with a log file. There are both off-the-shelf and open source tools available for file-integrity monitoring.
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.*	Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach. The log-review process does not have to be manual. Especially for those entities with a large number of servers, consider use of log harvesting, parsing, and alerting tools.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing back-up tapes off-site may result in longer time frames to restore data, perform analysis, and identify impacted systems or data.

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

Requirement	Guidance
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identity all wireless devices in use.	Implementation and/or exploitation of wireless technology within a network is one of the most common paths for malicious users to gain access to the network and cardholder data. If a wireless device or network is installed without a company's knowledge, it can allow an attacker to easily and "invisibly" enter the network. In addition to wireless analyzers, port scanners, and other network tools that detect wireless devices can be used. Due to the ease with which a wireless access point can be attached to a network, the difficulty in detecting their presence, and the increased risk presented by unauthorized wireless devices, these scans must be performed even when a policy exists prohibiting the use of wireless technology. An organization should have, as part of its incident response plan, documented procedures to follow in the event an unauthorized wireless access point is detected. A wireless IDS/IPS should be configured to automatically generate an alert, but the plan must also document response procedures if an unauthorized device is detected during a manual wireless scan.
11.2 Run internal and external network vulnerability scans 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). *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.*	A vulnerability scan is an automated tool run against external and internal network devices and servers, designed to expose potential vulnerabilities and identify ports in networks that could be found and exploited by malicious individuals. Once these weaknesses are identified, the entity corrects them, and repeats the scan to verify the vulnerabilities have been corrected. At the time of an entity's initial PCI DSS assessment, it is possible that four quarterly scans have not yet been performed. If the most recent scan result meets the criteria for a passing scan, and there are policies and procedures in place for future quarterly scans, the intent of this requirement is met. It is not necessary to delay an "in place" assessment for this requirement due to a lack of four scans if these conditions are satisfied.

Requirement	Guidance
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: **11.3.1** Network-layer penetration tests **11.3.2** Application-layer penetration tests.	Network and application penetration tests are different from vulnerability scans in that penetration tests are more manual, attempt to actually exploit some of the vulnerabilities identified in scans, and include techniques used by malicious individuals to take advantage of weak security systems or processes. Before applications, network devices, and systems are released into production, they should be hardened and secured using security best practices (per Requirement 2.2). Vulnerability scans and penetration tests will expose any remaining vulnerabilities that could later be found and exploited by an attacker.
11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	These tools compare the traffic coming into the network with known "signatures" of thousands of compromise types (hacker tools, Trojans and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection via these tools, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these tools should be monitored, so that the attempted intrusions can be stopped. There are thousands of compromise types, with more being discovered on a daily basis. Stale versions of these systems will not have current "signatures" and will not identify new vulnerabilities that could lead to an undetected breach. Vendors of these products provide frequent, often daily, updates.
11.5 Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least weekly. *Note: For file-integrity monitoring 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. 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).*	File-integrity monitoring (FIM) systems check for changes to critical files, and notify when such changes are detected. There are both off-the-shelf and open source tools available for file integrity monitoring. If not implemented properly and the output of the FIM monitored, a malicious individual could alter configuration file contents, operating system programs, or application executables. Such unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.

Guidance for Requirement 12: Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site

Requirement	Guidance
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following: **12.1.1** Addresses all PCI DSS requirements. **12.1.2** Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment. **12.1.3** Includes a review at least once a year and updates when the environment changes.	A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. A strong security policy sets the security tone for the whole company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. Security threats and protection methods evolve rapidly throughout the year. Without updating the security policy to reflect these changes, new protection measures to fight against these threats are not addressed.
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	Daily operational security procedures act as "desk instructions" for workers to use in their day-to-day system administrative and maintenance activities. Undocumented operational security procedures will lead to workers who are not aware of the full scope of their tasks, processes that cannot be repeated easily by new workers, and potential gaps in these processes that may allow a malicious individual to gain access to critical systems and resources.
12.3 Develop usage policies for critical employee-facing technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	Employee usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for employees as to correct usage and implementation. If usage policies are not in place, employees may use the technologies in violation of company policy, thereby allowing malicious individuals to gain access to critical systems and cardholder data. An example can be unknowingly setting up wireless networks with no security. To ensure that company standards are followed and only approved technologies are implemented, consider confining implementation to operations teams only and not allowing unspecialized/general employees install these technologies.

Requirement		Guidance
12.3.1	Explicit management approval	Without requiring proper management approval for implementation of these technologies, an employee may innocently implement a solution to a perceived business need, but also open a huge hole that subjects critical systems and data to malicious individuals.
12.3.2	Authentication for use of the technology	If technology is implemented without proper authentication (user IDs and passwords, tokens, VPNs, etc.), malicious individuals may easily use this unprotected technology to access critical systems and cardholder data.
12.3.3	List of all such devices and personnel with access	Malicious individuals may breach physical security and place their own devices on the network as a "back door." Employees may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations. Consider establishing an official naming convention for devices, and label and log all devices in concert with established inventory controls.
12.3.4	Labeling of devices with owner, contact information, and purpose	
12.3.5	Acceptable uses of the technologies	By defining acceptable business use and location of company-approved devices and technology, the company is better able to manage and control gaps in configurations and operational controls, to ensure a "back door" is not opened for a malicious individual to gain access to critical systems and cardholder data.
12.3.6	Acceptable network locations for the technologies	
12.3.7	List of company-approved products	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Remote-access technologies are frequent "back doors" to critical resources and cardholder data. By disconnecting remote-access technologies when not in use (for example, those used to support your systems by your POS or other vendors), access and risk to networks is minimized. Consider using controls to disconnect devices after 15 minutes of inactivity. Please also see Requirement 8.5.6 for more on this topic.
12.3.9	Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use	
12.3.10	When accessing cardholder data remotely via remote-access technologies, prohibit, copy, move, and storage of cardholder data onto local hard drives and removable electronic media.	To ensure your employees are aware of their responsibilities to not store or copy cardholder data onto their local personal computer or other media, your company should have a policy that clearly prohibits such activities.
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.

Requirement	Guidance
12.5 Assign to an individual or team the following information security management responsibilities: **12.5.1** Establish, document, and distribute security policies and procedures. **12.5.2** Monitor and analyze security alerts and information, and distribute to appropriate personnel. **12.5.3** Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. **12.5.4** Administer user accounts, including additions, deletions, and modifications. **12.5.5** Monitor and control all access to data.	Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data.
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	If users are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through employee errors or intentional actions.
12.6.1 Educate employees upon hire and at least annually.	If the security awareness program does not include annual refresher sessions, key security processes and procedures may be forgotten or bypassed, resulting in exposed critical resources and cardholder data.
12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.	Requiring an acknowledgement by employees (example: in writing or electronically) helps ensure that they have read and understood the security policies/procedures, and that they have made a commitment to comply with these policies.
12.7 Screen potential employees (see definition of "employees" at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. *For those employees 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*.	Performing thorough background investigations prior to hiring employees who are expected to be given access to cardholder data reduces the risk of unauthorized use of PANs and other cardholder data by individuals with questionable or criminal backgrounds. It is expected that a company would have a policy and process for background checks, including their own decision process for which background check results would have an impact on their hiring decisions (and what that impact would be).

Requirement		Guidance
12.8	If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	If a merchant or service provider shares cardholder data with a service provider, then certain requirements apply to ensure continued protection of this data will be enforced by such service providers.
12.8.1	Maintain a list of service providers.	Knowing who their service providers are identifies where potential risk extends to outside of the organization.
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients, and thus holds them accountable.
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider.
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status.	Knowing a service provider's PCI DSS compliance status provides further assurance that they comply with the same requirements that an organization is subjected to.
12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach.	Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities.

Requirement		Guidance
12.9.1	Create the incident response plan to be implemented in the event of system breach. Ensure 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 back-up 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	The incident response plan should be thorough and contain all the key elements to allow your company to respond effectively in the event of a breach that could impact cardholder data.
12.9.2	Test the plan at least annually.	Without proper testing, key steps may be missed that could limit exposure during an incident.
12.9.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become "polluted" by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation. If internal resources are not available, consider contracting with a vendor that provides these services.
12.9.4	Provide appropriate training to staff with security breach response responsibilities.	
12.9.5	Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	These monitoring systems are designed to focus on potential risk to data, are critical in taking quick action to prevent a breach, and must be included in the incident-response processes.

Requirement		Guidance
12.9.6	Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Incorporating “lessons learned” into the incident response plan after an incident helps keep the plan current and able to react to emerging threats and security trends.

Guidance for Requirement A.1: Additional PCI DSS Requirements for Shared Hosting Providers

Requirement A.1: Shared hosting providers protect cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including shared hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that shared hosting providers must protect each entity's hosted environment and data. Therefore, shared hosting providers must additionally comply with the requirements in this Appendix.

Requirement		Guidance
A.1	Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*	Appendix A of the PCI DSS is intended for shared hosting providers who wish to provide their merchant and/or service provider customers with a PCI DSS compliant hosting environment. These steps should be met, in addition to all other relevant PCI DSS requirements.
A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	If a merchant or service provider is allowed to run their own applications on the shared server, these should run with the user ID of the merchant or service provider, rather than as a privileged user. A privileged user would have access to all other merchants' and service providers' cardholder data environments as well as their own.
A.1.2	Restrict each entity's access and privileges to own cardholder data environment only.	To ensure that access and privileges are restricted such that each merchant or service provider only has access to their own cardholder data environment, consider the following: (1) privileges of the merchant's or service provider's web server user ID; (2) permissions granted to read, write, and execute files; (3) permissions granted to write to system binaries; (4) permissions granted to merchant's and service provider's log files; and (5) controls to ensure one merchant or service provider cannot monopolize system resources.
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	Logs should be available in a shared hosting environment, so the merchants and service providers have access to, and can review, logs specific to their cardholder data environment.

Requirement		Guidance
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	Shared hosting providers must have processes to provide quick and easy response in the event that a forensic investigation is needed for a compromise, down to the appropriate level of detail so that an individual merchant's or service provider's details are available.

Appendix A: PCI Data Security Standard: Related Documents

The following documents were created to assist merchants and service providers in understanding the PCI Data Security Standard and compliance requirements and responsibilities.

Document	Audience
PCI Data Security Standard Requirements and Security Assessment Procedures	All merchants and service providers
Navigating PCI DSS: Understanding the Intent of the Requirements	All merchants and service providers
PCI Data Security Standard: Self-Assessment Questionnaire Guidelines and Instructions	All merchants and service providers
PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation	Merchants[10]
PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation	Merchants[10]
PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation	Merchants[10]
PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation	Merchants[10] and all service providers
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	All merchants and service providers

[10] To determine the appropriate Self-Assessment Questionnaire, see *PCI Data Security Standard: Self-Assessment Questionnaire Guidelines and Instructions*, "Selecting the SAQ and Attestation That Best Apply to Your Organization."