Payment Card Industry (PCI)
Data Security Standard

Navigating PCI DSS

Understanding the Intent of the Requirements

Version 2.0

October 2010

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.*
October 28, 2010	*2.0*	*To align content with new PCI DSS v2.0.*

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 onsite assessment or Self Assessment Questionnaire (SAQ), the *PCI DSS Requirements and Security Assessment Procedures* and the *PCI DSS Self-Assessment Questionnaires 2.0* are the documents of record.

PCI DSS requirements apply to all system components. In the context of PCI DSS, "system components" are defined as any network component, server or application that is included in, or connected to, the cardholder data environment. System components" also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. The cardholder data environment is comprised of people, processes and technology that handle cardholder data or sensitive authentication data.

- 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, application, 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 (for example, Internet) applications.

The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.
- The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate an entity's network is not a PCI DSS requirement. However, it is strongly recommended as a method that 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 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.

Virtualization

If virtualization is implemented, all components within the virtual environment will need to be identified and considered in scope for the review, including the individual virtual hosts or devices, guest machines, applications, management interfaces, central management consoles, hypervisors, etc. All intra-host communications and data flows must be identified and documented, as well as those between the virtual component and other system components.

The implementation of a virtualized environment must meet the intent of all requirements, such that the virtualized systems can effectively be regarded as separate hardware. For example, there must be a clear segmentation of functions and segregation of networks with different security levels; segmentation should prevent the sharing of production and test/development environments; the virtual configuration must be secured such that vulnerabilities in one function cannot impact the security of other functions; and attached devices, such as USB/serial devices, should not be accessible by all virtual instances.

Additionally, all virtual management interface protocols should be included in system documentation, and roles and permissions should be defined for managing virtual networks and virtual system components. Virtualization platforms must have the ability to enforce separation of duties and least privilege, to separate virtual network management from virtual server management.

Special care is also needed when implementing authentication controls to ensure that users authenticate to the proper virtual system components, and distinguish between the guest VMs (virtual machines) and the hypervisor.

Cardholder Data and Sensitive Authentication Data Elements

PCI DSS applies wherever account data is stored, processed or transmitted. *Account Data* consists of *Cardholder Data* plus *Sensitive Authentication Data*, as follows:

Cardholder Data includes:	***Sensitive Authentication Data includes:***
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full magnetic stripe data or equivalent data on a chip • CAV2/CVC2/CVV2/CID • PINs/PIN blocks

The primary account number is the defining factor in the applicability of PCI DSS requirements. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.

If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements ***except*** Requirements 3.3 and 3.4, which apply only to PAN.

PCI DSS represents a minimum set of control objectives which may be enhanced by local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personally identifiable information or other data elements (for example, cardholder name), or define an entity's disclosure practices related to consumer information. Examples include legislation related to consumer data protection, privacy, identity theft, or data security. PCI DSS does not supersede local or regional laws, government regulations or other legal requirements.

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; but is presented to illustrate the different type of requirements that apply to each data element.

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	**Cardholder Data**	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data [1]	Full Magnetic Stripe Data [2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

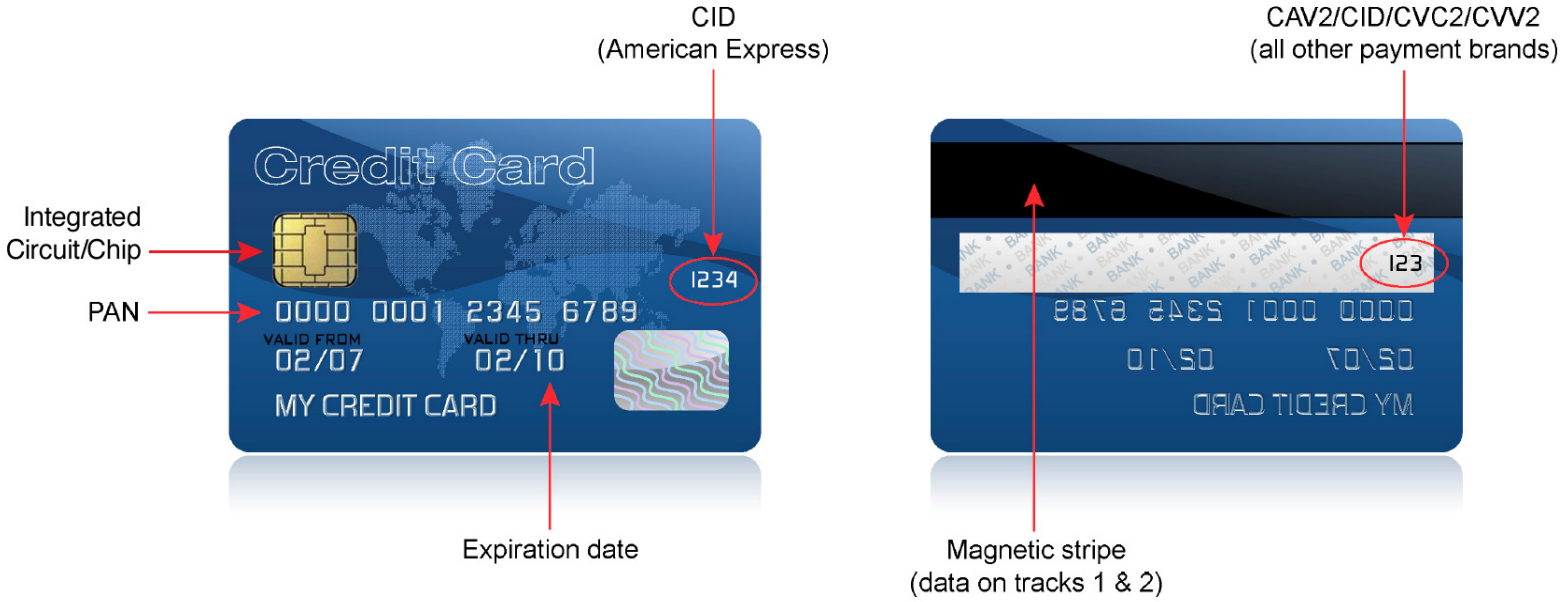
PCI DSS ***applies only*** if PANs are stored, processed and/or transmitted.

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

2 Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

Location of Cardholder Data and Sensitive Authentication Data

Sensitive authentication data consists of magnetic stripe (or track) data[3], card validation code or value[4], and PIN data[5]. **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.



Note: *The chip contains track equivalent data as well as other sensitive data, including the Integrated Circuit (IC) Chip Card Verification Value (also referred to Chip CVC, iCVV, CAV3 or iCSC).*

---

3 Data encoded in the magnetic stripe used for authorization during a card-present transaction. This data may also be found on a 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.

4 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.

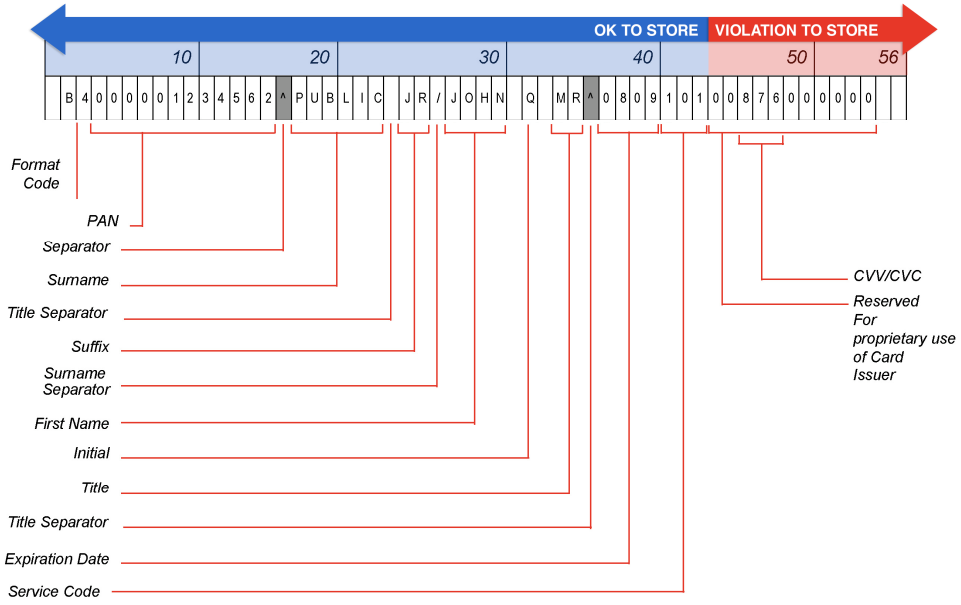
5 Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

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.

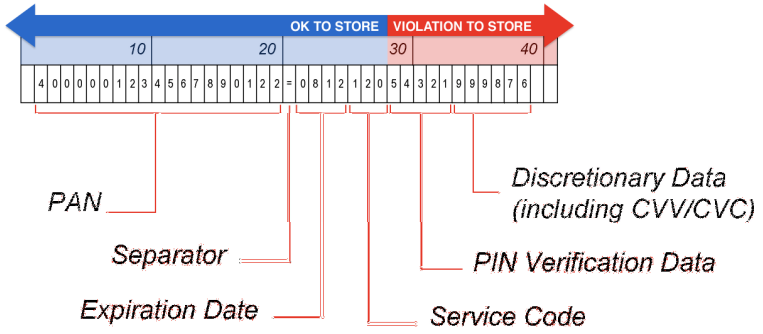
Track 1

- Contains all fields of both track 1 and track 2
- Length up to 79 characters



Track 2

- Shorter processing time for older dial-up transmissions
- Length up to 40 characters



***Note**: Discretionary Data fields are defined by the card issuer and/or payment card brand. Issuer-defined fields containing data that are not considered by the issuer/payment brand to be sensitive authentication data may be included within the discretionary data portion of the track, and it may be permissible to store this particular data under specific circumstances and conditions, as defined by the issuer and/or payment card brand.*

However, any data considered to be sensitive authentication data, whether it is contained in a discretionary data field or elsewhere, may not be stored after authorization.

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 or programs

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 for all personnel

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

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, employee Internet access through desktop browsers, employee e-mail access, dedicated connections 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.

Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

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. Virtual environments where data flows do not transit a physical network should be assessed to ensure appropriate network segmentation is achieved.
1.1.1 A formal process for approving and testing all 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. Data flows between virtual machines should be included in policy and process.

Requirement	Guidance
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. Network and data flow diagrams should include virtual system components and document Intra-host data flows.
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. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.	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.

Requirement	Guidance
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.
1.2 Build firewall and router configurations that restrict 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 system component with (at a minimum) stateful inspection firewall capability, 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 firewall functionality 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 run these files only 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.

Requirement	Guidance
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	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. Firewalls must be installed between all wireless networks and the CDE, regardless of the purpose of the environment to which the wireless network is connected. This may include, but is not limited to, corporate networks, retail stores, warehouse environments, etc.
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, process or transmit cardholder data). If direct access is allowed between public systems and the CDE, 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 traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	The DMZ is that part of the network that manages connections between the Internet (or other untrusted networks), 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. This functionality 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.
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	Termination of IP connections at the DMZ provides opportunity for inspection and restriction of source/destination, and/or inspection / blocking of content, thus preventing unfiltered access between untrusted and trusted environments.
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	Termination of IP connections both inbound and outbound provides opportunity for inspection and restriction of source/destination, and/or inspection / blocking of content, thus preventing unfiltered access between untrusted and trusted environments. This helps prevent, for example, malicious individuals from sending data they've obtained from within your network out to an external untrusted server in an untrusted network.

Requirement	Guidance
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 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	All traffic outbound from inside the cardholder data environment should be evaluated to ensure that outbound traffic follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content). Where environments have no inbound connectivity allowed, outbound connections may be achieved via architectures or system components that interrupt and inspect the IP connectivity.
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 system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	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. ***Note:*** *the intent of this requirement does not include storage in volatile memory.*

Requirement	Guidance
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note**: Methods to obscure IP addressing may include, but are not limited to:* ▪ *Network Address Translation (NAT)* ▪ *Placing servers containing cardholder data behind proxy servers/firewalls or content caches,* ▪ *Removal or filtering of route advertisements for private networks that employ registered addressing,* ▪ *Internal use of RFC1918 address space instead of registered addresses.*	Restricting the broadcast of IP addresses is essential to prevent a hacker "learning" the IP addresses of the internal network, and using that information to access the network. Effective means to meet the intent of this requirement may vary depending on the specific networking technology being used in your environment. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks. One technique to prevent IP address information from being discovered on an IPv4 network is to implement Network Address translation (NAT). NAT, which is typically managed by the firewall, allows an organization to have internal addresses that are visible only 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. For IPv4 networks, the RFC1918 address space is reserved for internal addressing, and should not be routable on the Internet. As such, it is preferred for IP addressing of internal networks. However, organizations may have reasons to utilize non-RFC1918 address space on the internal network. In these circumstances, prevention of route advertisement or other techniques should be used to prevent internal address space being broadcast on the Internet or disclosed to unauthorized parties.
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. ***Note:** The intent of this requirement applies to remote access computers regardless of whether they are employee owned or company owned. Systems that cannot be managed by corporate policy introduce weaknesses to the perimeter and provide opportunities that malicious individuals may exploit.*

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

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

Requirement	Guidance
2.1 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to 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**.**	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 (for example, 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. Sources of industry-accepted system hardening standards may include, but are not limited to: ▪ Center for Internet Security (CIS) ▪ International Organization for Standardization (ISO) ▪ SysAdmin Audit Network Security (SANS) ▪ National Institute of Standards Technology (NIST)	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. Source websites where you can learn more about industry best practices that can help you implement configuration standards include, but are not limited to: www.nist.gov, www.sans.org, www.cisecurity.org, www.iso.org. System configuration standards must also be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.

Requirement	Guidance
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	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 all servers within the cardholder data environment (usually Unix, Linux, or Windows based). This requirement may not apply to systems which have the ability to natively implement security levels on a single server (e.g. mainframe). Where virtualization technologies are used, each virtual component (e.g. virtual machine, virtual switch, virtual security appliance, etc.) should be considered a "server" boundary. Individual hypervisors may support different functions, but a single virtual machine should adhere to the "one primary function" rule. Under this scenario, compromise of the hypervisor could lead to the compromise of all system functions. Consequently, consideration should also be given to the risk level when locating multiple functions or components on a single physical system.
2.2.2 Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure. For example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	As stated in Requirement 1.1.5, 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 only the necessary services and protocols are enabled and that all insecure services and protocols are adequately secured before 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).

Requirement	Guidance
2.3 Encrypt all non-console administrative access using strong cryptography. 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.
2.4 Shared hosting providers must protect each entity's hosted environment and cardholder 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 methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other 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 unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the PCI 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 by implementing data retention and disposal policies, procedures and processes, as follows. **3.1.1** Implement a data retention and disposal policy that includes: ▪ Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements ▪ Processes for secure deletion of data when no longer needed ▪ Specific retention requirements for cardholder data ▪ A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements	A formal data retention policy identifies what data needs to be retained, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. In order to define appropriate retention requirements, an entity first needs to understand their own business needs as well as any legal or regulatory obligations that apply to their industry, and/or that apply to the type of data being retained. Extended storage of cardholder data that exceeds business need creates an unnecessary risk. The only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. Implementing secure deletion methods ensure that the data cannot be retrieved when it is no longer needed. **Remember, if you don't need it, don't store it!**

Requirement	Guidance
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: ***Note:*** *it is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.*	Sensitive authentication data consists of magnetic stripe (or track) data[6], card validation code or value[7], and PIN data[8]. **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." ***Note:*** *It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience.* *Any such data must be stored securely and in accordance with PCI DSS and specific payment brand requirements.*
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). 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* ▪ *Service code* *To minimize risk, store only these data elements as needed for business.*	If full track data is stored, malicious individuals who obtain that data can reproduce and sell payment cards.

[6] Data encoded in the magnetic stripe used for authorization during a card-present transaction. This data may also be found on a 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.

[7] 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.

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

Requirement	Guidance
3.2.2 Do not store the card-verification 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.	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).
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 legitimate business 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. This requirement relates to protection of PAN displayed on screens, paper receipts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when stored in files, databases, etc.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography (hash must be of the entire PAN) ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN) ▪ Index tokens and pads (pads must be securely stored) ▪ Strong cryptography with associated key-management processes and procedures ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*	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 them) in logs. By correlating hashed and truncated versions of a given PAN, a malicious individual may easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable. Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography."

Requirement	Guidance
▪ One-way hashes based on strong cryptography (hash must be of the entire PAN)	One-way hash functions such as the Secure Hash Algorithm (SHA) 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). To complicate the creation of rainbow tables it is recommended, but not a requirement, that a salt value be input to the hash function in addition to the PAN.
▪ Truncation (hashing cannot be used to replace the truncated segment of PAN)	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.). This requirement relates to protection of PAN when *stored* in files, databases, etc., and is not to be confused with Requirement 3.3 for protection of PAN displayed on screens, paper 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.
▪ Strong cryptography with associated key-management processes and procedures	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.

Requirement	Guidance
3.5 Protect any keys used to secure cardholder data against disclosure and misuse: ***Note**: This requirement also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. Key-encrypting keys, if used, must be at least as strong as the data-encrypting key in order to ensure proper protection of the key that encrypts the data as well as the data encrypted with that key. The requirement to protect keys from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures. Methods for secure storage of key-encrypting keys include but are not limited to hardware security modules (HSMs) and tamper evident storage with dual control and split knowledge.
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. It is not intended that the key-encrypting keys be encrypted, however they are to be protected against disclosure and misuse as defined in Requirement 3.5. Storing key-encrypting keys in physically and/or logically separate locations from data-encrypting keys reduces the risk of unauthorized access to both keys.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the **following:** ***Note:** Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	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, is based on industry standards and 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).

Requirement	Guidance
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, *NIST Special Publication 800-57*).	A cryptoperiod is the time span during which a particular cryptographic key can be used for its defined purpose. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimize the risk of someone's obtaining the encryption keys, and being able to decrypt data. If provided by encryption application vendor, follow the vendor's documented processes or recommendations for periodic changing of keys. The designated key owner or custodian can also refer to industry best practices on cryptographic algorithms and key management, for example *NIST Special Publication 800-57,* for guidance on the appropriate cryptoperiod for different algorithms and key lengths. The intent of this requirement applies to keys used to encrypt stored cardholder data, and any respective key-encrypting keys.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. ***Note**: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should be used only for decryption/verification purposes.*	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 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). ***Note:** Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	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 applicable for manual key management operations, or where key management is not implemented by the encryption product.
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.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	This process will ensure individuals that act as key custodians commit to the key-custodian role and understand the 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 continue to be 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 (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:* ▪ *The Internet* ▪ *Wireless technologies,* ▪ *Global System for Mobile communications (GSM)* ▪ *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. For example, Secure Sockets Layer (SSL) encrypts web pages and the data entered into them. When using SSL secured websites, ensure "https" is part of the URL. Note that some protocol implementations (such as SSL version 2.0 and SSH version 1.0) have documented vulnerabilities, such as buffer overflows, that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure configurations and versions to prevent an insecure connection being used.
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. ***Note**: The use of WEP as a security control was prohibited as of 30 June 2010.*	Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can limit 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. Examples of wireless implementations requiring strong cryptography include but are not limited to GPRS, GSM, WIFI, satellite, and Bluetooth. Strong cryptography 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 encryption should never be used as the sole means of encrypting data over a wireless channel since it is not considered strong cryptography, it is vulnerable due to weak initialization vectors in the WEP key-exchange process, and it lacks required key rotation. An attacker can use freely available brute-force cracking tools to easily penetrate WEP encryption. Current wireless devices should be upgraded (example: upgrade access point firmware to WPA2) to support strong encryption. If current devices cannot be upgraded, new equipment should be purchased or other compensating controls implemented to provide strong encryption.

Requirement	Guidance
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	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 provide strong encryption.

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 employee 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. If another type of solution addresses the identical threats with a different methodology than a signature-based approach, it may still be acceptable to meet the requirement. 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 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. Thus, it is imperative that anti-virus software be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

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 are protected from known vulnerabilities by having 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.

Requirement	Guidance
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. ***Notes**:* *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.* *The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.*	The intention of this requirement is that organizations keep up-to-date with new vulnerabilities that may impact their environment. While it is important to monitor vendor announcements for news of vulnerabilities and patches related to their products, it is equally important to monitor common industry vulnerability news groups and mailing lists for vulnerabilities and potential workarounds that may not yet be known or resolved by the vendor. Once an organization identifies a vulnerability that could affect their environment, the risk that vulnerability poses must be evaluated and ranked. This implies that the organization has some method in place to evaluate vulnerabilities and assign risk rankings on a consistent basis. While each organization will likely have different methods for evaluating a vulnerability and assigning a risk rating based on their unique CDE, it is possible to build upon common industry accepted risk ranking systems, for example CVSS. 2.0, NIST SP 800-30, etc. Classifying the risks (for example, as "high", "medium", or "low") allows organizations to identify and address high priority risk items more quickly, and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.
6.3 Develop software applications (internal and external, and including web-based administrative access to 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.
6.3.1 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 is 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
6.3.2 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. Code reviews can be conducted by knowledgeable internal personnel or third parties. 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. Code reviews may be performed manually, or with the assistance of automated review tools. Automated review tools have functionality that reviews code for common coding mistakes and vulnerabilities. While automated review is useful, it should not generally be relied upon as the sole means of code review. An individual knowledgeable and experienced in code review should be involved in the review process in order to identify code issues that are difficult or even impossible for an automated tool to identify. Assigning code reviews to someone other than the developer of the code allows an independent, objective review to be performed.
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	Without proper change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.
6.4.1 Separate development/test and production environments	Due to the constantly changing state of development and test environments, they tend to be less secure than the production environment. Without adequate separation between environments it may be possible for the production environment, and cardholder data, to be compromised due to vulnerabilities in a test or development environment.
6.4.2 Separation of duties between development/test and production environments	Reducing the number of personnel with access to the production environment and cardholder data minimizes risk and helps ensure that access is limited to those individuals with a business need to know. The intent of this requirement is to ensure that development/test functions are separated from production functions. For example, a developer may use an administrator-level account with elevated privileges for use in the development environment, and have a separate account with user-level access to the production environment. In environments where one individual performs multiple roles (for example application development and implementing updates to production systems), duties should be assigned such that no one individual has end-to-end control of a process without an independent checkpoint. For example, assign responsibility for development, authorization and monitoring to separate individuals.

Requirement	Guidance
6.4.3 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). Payment card brands and many acquires are able to provide account numbers suitable for testing in the event that you need realistic PANs to test system functionality prior to release.
6.4.4 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.
6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	Without proper change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced. Likewise, a change may negatively affect security functionality of a system necessitating the change to be backed out.
6.4.5.1 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.
6.4.5.2 Documented change approval by authorized parties.	Approval by authorized parties indicates that the change is a legitimate and approved change sanctioned by the organization.
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	Thorough testing should be performed to verify that the security of the environment is not reduced by implementing a change. Testing should validate that all existing security controls remain in place, are replaced with equally strong controls, or are strengthened after any change to the environment. For custom code changes, testing includes verifying that no coding vulnerabilities have been introduced by the change.
6.4.5.4 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 applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: ***Note**: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices 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. As with all PCI DSS requirements, Requirements 6.5.1 through 6.5.5 and 6.5.7 through 6.5.9 are the *minimum* controls that should be in place. This list is composed of the most common, accepted secure coding practices at the time that this version of the PCI DSS was published. As industry accepted secure coding practices change, organizational coding practices should likewise be updated to match. The examples of secure coding resources provided (SANS, CERT, and OWASP) are suggested sources of reference and have been included for guidance only. An organization should incorporate the relevant secure coding practices as applicable to the particular technology in their environment.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection**,** 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 a commonly used method for compromising 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 requests should be validated before being sent to the application – for example, by checking for all alpha characters, mix of alpha and numeric characters, etc.
6.5.2 Buffer overflow	Ensure that applications are not vulnerable to buffer overflow attacks. Buffer overflows happen when an application does not have appropriate bounds checking on its buffer space. To exploit a buffer overflow vulnerability, an attacker would send an application a larger amount of information than one of its particular buffers is able to handle. This can cause the information in the buffer to be pushed out of the buffer's memory space and into executable memory space. When this occurs, the attacker has the ability to insert malicious code at the end of the buffer and then push that malicious code into executable memory space by overflowing the buffer. The malicious code is then executed and often enables the attacker remote access to the application and/or infected system.
6.5.3 Insecure cryptographic storage	Prevent cryptographic flaws. Applications that do not utilize strong cryptographic functions properly to store data are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain clear-text access to encrypted data.

Requirement	Guidance
6.5.4 Insecure communications	Properly encrypt all authenticated and sensitive communications. Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain control of an application or even gain clear-text access to encrypted data.
6.5.5 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 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."
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). ***Note**: This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.*	Any high vulnerabilities noted per Requirement 6.2 that could affect the application should be accounted for during the development phase. For example, a vulnerability identified in a shared library or in the underlying operating system should be evaluated and addressed prior to the application being released to production.
For web applications and application interfaces (internal or external), the following additional requirements apply:	Web applications, both internally and externally (public) facing, have unique security risks based upon their architecture as well as their relative ease and occurrence of compromise.
6.5.7 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.

Requirement	Guidance
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, and directory traversal)	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. Consistently enforce access control in presentation layer and business logic for all URLs. Frequently, the only way an application protects sensitive functionality is 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. Protect against directory traversal. An attacker may be able to enumerate and navigate the directory structure of a website thus gaining access to unauthorized information as well as gaining further insight into the workings of the site for later exploitation.
6.5.9 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.
6.6 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.

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 a documented approval by authorized parties specifying 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 "least privilege" and "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. Role based access control enforcement is not limited to an application layer or any specific authorization solution. For example, technology including but not limited to directory services such as Active Directory or LDAP, Access Control Lists (ACLs), and TACACS are viable solutions as long as they are appropriately configured to enforce the principles of least privilege and need to know. Organizations 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, including appropriate management authorization processes.
7.2 Establish an access control system for systems 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: **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 ***Note:*** *Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*	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.

***Note:** These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*

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**:** ▪ Something you know, such as a password or passphrase ▪ Something you have, such as a token device or smart card ▪ Something you are, such as a biometric	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). A digital certificate is a valid option as a form of the authentication type "something you have" as long as it is unique.

Requirement	Guidance
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. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) ***Note**: Two-factor authentication requires that two of the three authentication methods (see Req. 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.*	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). This requirement is intended to apply to users that have remote access to the network, where that remote access could lead to access to the cardholder data environment. In this context, remote access refers to network-level access originating from outside an entity's own network, either from the Internet or from an "untrusted" network or system, such as a third party or an employee accessing the entity's network using his/her mobile computer. Internal LAN-to-LAN access (for example, between two offices via secure VPN) is not considered remote access for the purposes of this requirement. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, two-factor authentication for remote access to that network would not required by PCI DSS. However, two-factor authentication is required for any remote access to networks with access to the cardholder data environment, and is recommended for all remote access to the entity's networks.
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	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. During transmission, the user credentials can be encrypted or the tunnel can be encrypted
8.5 Ensure proper user identification and authentication 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 identification and authentication management.
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.

Requirement	Guidance
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 passwords for first-time use and resets 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 Human Resources 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 access only during the time period needed. Monitor vendor remote access accounts when in use.	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. Monitoring of vendor access to the cardholder data environment applies in the same way as it does for other users, such as organizational personnel. This includes monitoring and logging of activities as required by PCI DSS Requirements 10.1 and 10.2, and verifying that usage of vendor remote accounts is in accordance with the policy as defined in Requirements 12.3.8 and 12.3.9.
8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	Communicating password/authentication 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, or other authentication methods.	If multiple users share the same authentication credentials (for example, user 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 has knowledge of the authentication credentials. This requirement for unique IDs and complex passwords is often met within administrative functions by using, for example, sudo or SSH such that the administrator initially logs on with their own unique ID and password, and then connects to the administrator account via sudo or SSH. Often direct root logins are disabled to prevent use of this shared administrative account. This way, individual accountability and audit trails are maintained. However, even with use of tools such as sudo and SSH, the actual administrator IDs and passwords should also meet PCI DSS requirements (if such accounts are not disabled) to prevent them from being misused.
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-authenticate to re-activate the terminal or session.	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. Restrict user direct access or queries to databases to database administrators.	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. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

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 and/or access control mechanisms to monitor individual physical 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, process, or transmit 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 sensitive areas storing cardholder data. Examples of sensitive areas include corporate database server rooms, back-end server room of a retail location that stores cardholder data, and storage areas for large quantities of cardholder data,
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is explicitly authorized.	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, handheld devices, networking/ communications hardware, and telecommunication lines.	Without security over access to wireless components and devices, malicious users could use your organization's unattended wireless devices to access your network resources, or even connect their own devices to your wireless network to gain unauthorized access. Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to your wired network resources. Consider placing wireless access points, gateways and networking/ communications hardware in secure storage areas, such as within locked closets or server rooms. For wireless networks, ensure strong encryption is enabled. Also consider enabling 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 easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	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. Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas containing 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	Visitor controls are important to ensure visitors only enter areas they are authorized to enter, that they are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	
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 onsite personnel 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 back-ups in a secure location, preferably 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.
9.6 Physically secure all media.	Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk.
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	Procedures and processes help protect 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.
9.7.1 Classify media so the sensitivity of the data can be determined.	It is important that media be identified such that its classification status can be easily discernable. Media not identified as confidential may not be adequately protected or may be lost or stolen.

Requirement	Guidance
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 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.
9.9 Maintain strict control over the storage and accessibility of media.	Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.
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 or at all.
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	If steps are not taken to destroy information contained on hard disks, portable drives, CD/DVDs, or paper prior to disposal, malicious individuals may be able to retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as “dumpster diving,” where they search through trash cans and recycle bins looking for information they can use to launch an attack. Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).
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, if not impossible, 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:	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. Logging of the following events enables an organization to identify and trace potentially malicious activities.
10.2.1 All individual accesses to cardholder data	Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new, unauthorized account in order to access cardholder data. A record of all individual accesses to cardholder data can identify which accounts may have been compromised or misused.
10.2.2 All actions taken by any individual with root or administrative privileges	Accounts with increased privileges, such as the “administrator” or “root” account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.
10.2.3 Access to all audit trails	Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account,
10.2.4 Invalid logical access attempts	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user’s attempts to “brute force” or guess a password.

Requirement	Guidance
10.2 5 Use of identification and authentication mechanisms	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts which may be used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account. Activities including, but not limited to, escalation of privilege or changes to access permissions may indicate unauthorized use of a system's authentication mechanisms.
10.2.6 Initialization of the audit logs	Turning the audit logs off prior to performing illicit activities is a common goal for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions.
10.2.7 Creation and deletion of system-level objects	Malicious software, such as malware, often creates or replaces system level objects on the target system in order to control a particular function or operation on that system. Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "system-level objects".
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 details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.

Requirement	Guidance
10.4 Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note**: One example of time synchronization technology is Network Time Protocol (NTP).* **10.4.1** Critical systems have the correct and consistent time **10.4.2** Time data is protected **10.4.3** Time settings are received from industry-accepted time sources	Time synchronization technology is used to synchronize clocks on multiple systems. When properly deployed, this technology can synchronize clocks on large numbers of systems to within a fraction of a second of each other. Some problems that can occur when clocks are not properly synchronized include but are not limited to, making it difficult if not impossible to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach), and preventing cryptographic protocols such as SSH that rely on absolute time from functioning properly. For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised. In order to ensure consistent time, ideally there should be only a few internal (central) time servers within an entity. These servers receive UTC (Coordinated Universal Time) data directly from reliable, known external time servers, via special radio, GPS satellites, or other external network source, and peer with each other to ensure they keep accurate time. Other systems then receive the time from these servers. 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. A malicious individual may also try to directly change the clock on a system component to hide their presence – for example, by changing the system clock to an earlier time. For these reasons, it is important that time is accurate on all systems and that time data is protected against unauthorized access and changes. Time data includes the parameters and methods used to set each system's clock. More information on NTP can be found at *www.ntp.org*, including information about time, time standards, and servers.
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 or 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 and detect unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	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. Unauthorized wireless devices may be hidden within or attached to a computer or other system component, or be attached directly to a network port or network device, such as a switch or router. Any such unauthorized device could result in an unauthorized access point into the environment. 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 processes must be performed even when a policy exists prohibiting the use of wireless technology. The size and complexity of a particular environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment. For example: In the case of a single standalone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, performing a detailed physical inspection of the kiosk itself may be sufficient to provide assurance that a rogue wireless access point has not been attached or installed. However, in an environment with multiple nodes (such as in a large retail store, call centre, server room or data center), it becomes more difficult to perform a detailed physical inspection due to the number of system components and network points where a rogue wireless access device could be installed or hidden. In this case, multiple methods may be combined to meet the requirement, such as performing physical system inspections in conjunction with the results of a wireless analyzer. Network access control (NAC) solutions can perform device authentication and configuration management to prevent unauthorized systems connecting to the network, or unauthorized devices connecting to authorized systems on the network. 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.

Requirement	Guidance
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:*** *It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.*	A vulnerability scan is an automated tool run against external and internal network devices and servers, designed to expose potential vulnerabilities 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.
11.2.1 Perform quarterly internal vulnerability scans.	An established process for identifying vulnerabilities on internal systems within the CDE requires that vulnerability scans be conducted quarterly. Identifying and addressing vulnerabilities in a timely manner reduces the likelihood of a vulnerability being exploited and potential compromise of a system component or cardholder data. Vulnerabilities posing the greatest risk to the environment (for example, ranked "High" per Requirement 6.2) should be resolved with the highest priority. As internal networks may be constantly changing during the year, it is possible that an entity may not have consistently clean internal vulnerability scans. The intent is for an entity to have a robust vulnerability management program in place to resolve noted vulnerabilities in a reasonable timeframe. At minimum, "High" vulnerabilities must be addressed in a timely fashion. Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a firewall administrator should not be responsible for scanning the firewall), or an entity may choose to have internal vulnerability scans performed by a PCI SSC Approved Scanning Vendor (ASV), QSA or other firm specializing in vulnerability scanning.

Requirement	Guidance
11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.*	As external networks are at greater risk of compromise, quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV). ASVs are required to follow a set of scanning and reporting criteria set forth by the PCI SSC in the Approved Scanning Vendor Program Guide.
11.2.3 Perform internal and external scans after any significant change. ***Note:*** *Scans conducted after changes may be performed by internal staff.*	Scanning an environment after any significant changes are made ensures that changes were completed appropriately such that the security of the environment was not compromised as a result of the change. It may not be necessary to scan the entire environment after a change. However, all system components affected by the change will need to be scanned.
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	The intent of a penetration test is to simulate a real world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process which may include exploiting identified vulnerabilities. Often, performing a vulnerability scan is one of the first steps a penetration tester will perform in order to comprise a strategy of attack, although it is not the only step. Even if a vulnerability scan does not detect any known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is generally a highly manual process. While some automated tools may be used, the tester must utilize their knowledge of systems to penetrate into an environment. Often the tester will chain several types of exploits together with a goal of breaking through layers of defenses. For example, if the tester finds a means to gain access to an application server, they will then use the compromised server as a point to stage a new attack based on the resources the server has access to. In this way a tester is able to simulate the methods performed by an attacker in order to identify any areas of potential weakness in the environment that need to be addressed.

Requirement	Guidance
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	Intrusion detection and/or intrusion prevention systems (IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors 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. IDS/IPS devices should be implemented such that they monitor inbound and outbound traffic at the perimeter of the CDE as well as at critical points within the CDE. Critical points inside the CDE may include database servers storing cardholder data, cryptographic key storage locations, processing networks, or other sensitive system components, as determined by an entity's environment and as documented in their risk assessment. While many IDS/IPS devices today are able to monitor multiple points inside of the CDE via one device, it is important to remember the increased exposure that may occur as a result of a failure in that single device. Thus, it is important to incorporate appropriate redundancy in the IDS/IPS infrastructure. There are thousands of compromise types, with more being discovered on a daily basis. Stale signatures and scanning engines on IDS/IPS devices will not have the ability to identify new vulnerabilities that could lead to an undetected breach. Vendors of these products provide frequent, often daily, updates that should be evaluated and applied on a regular basis.
11.5 Deploy file-integrity monitoring tools 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) tools 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 all personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

Requirement	Guidance
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following: **12.1.1** Addresses all PCI DSS requirements.	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 personnel know what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. (Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.)	A risk assessment enables an organization to identify threats and the associated vulnerabilities which have the potential to negatively impact their business. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized. Performing risk assessments at least annually allows the organization to keep up to date with organizational changes and evolving threats, trends and technologies,
12.1.3 Includes a review at least annually and updates when the environment changes.	Security threats and protection methods evolve rapidly throughout the year. Without updating the security policy to reflect relevant 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 personnel to use in their day-to-day system administrative and maintenance activities. Undocumented operational security procedures will lead to personnel 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.

Requirement	Guidance
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	Personnel usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for personnel as to correct usage and implementation. If usage policies are not in place, personnel 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 personnel install these technologies.
12.3.1 Explicit approval by authorized parties	Without requiring proper approval for implementation of these technologies, individual personnel 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 A 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." Personnel 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. Also, logical labeling may be employed with information such as codes that can correlate the device to its owner, contact information and purpose.
12.3.4 Labeling of devices to determine owner, contact information and purpose	
12.3.5 Acceptable uses of the technology	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 vendor, other vendors, or business partner), 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 and business partners only when needed by vendors and business partners, with immediate deactivation after use	

Requirement	Guidance
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	To ensure all personnel are aware of their responsibilities to not store or copy cardholder data onto their local personal computer or other media, your policy should clearly prohibit such activities except for personnel that have been explicitly authorized to do so. Any such authorized personnel are responsible for ensuring that cardholder data in their possession is handled in accordance with all PCI DSS requirements, as that remote personnel's environment is now considered a part of the organization's cardholder data environment.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel	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.
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 personnel aware of the importance of cardholder data security.	If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.

Requirement	Guidance
12.6.1 Educate personnel upon hire and at least annually. ***Note:*** *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	If the security awareness program does not include periodic refresher sessions, key security processes and procedures may be forgotten or bypassed, resulting in exposed critical resources and cardholder data. The focus and depth of the initial and refresher training can vary depending on the role of the personnel, and should be tailored as appropriate for the particular audience. For example, sessions for database administrators may be focused on specific technical controls and processes, while training for retail cashiers may focus on secure transaction procedures Consider including ongoing awareness updates to keep employees up to date with current policies and procedures. The method of delivery may also vary to suit the particular audience or training being delivered. For example, initial and annual training may be delivered via a formal hands-on or computer-based training session, while ongoing periodic updates may be delivered via e-mails, posters, newsletters, etc.
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Requiring an acknowledgement by personnel in writing or electronically helps ensure that they have read and understood the security policies/procedures, and that they have made and will continue to make a commitment to comply with these policies.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history and reference checks.) ***Note****: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	Performing thorough background investigations prior to hiring potential personnel 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). To be effective, the level of background checking should be appropriate for the particular position. For example, positions requiring greater responsibility or that have administrative access to critical data or systems may warrant more detailed background checks than positions with less responsibility and access. It may also be appropriate for the process to cover internal transfers, where personnel in lower risk positions, and who have not already undergone a detailed background check, are promoted or transferred to positions of greater responsibility or access.
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.	Keeping track of all service providers identifies where potential risk extends to outside of the organization.

Requirement	Guidance
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 at least annually.	Knowing your service providers' PCI DSS compliance status provides assurance that they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement applies only to those services actually delivered to the client, and only those services in scope for the client's PCI DSS assessment. For example, if a provider offers firewall/IDS and ISP services, a client who utilizes only the firewall/IDS service would only include that service in the scope of their PCI DSS assessment.
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.
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.

Requirement	Guidance
12.9.2 Test the plan at least annually.	Without proper testing, key steps may be missed which could result in increased exposure during an incident. If within the last year the incident response plan was activated in its entirety, covering all components of the plan, a detailed review of the actual incident and its response may be sufficient to provide a suitable test. If only some components of the plan were recently activated, the remaining components would still need to be tested. If no components of the plan were activated in the last 12 months, the annual test would need to encompass all components of the plan.
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.
12.9.6 Develop a 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 has access only 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.
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	Eligible Merchants[9]
PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation	Eligible Merchants[9]
PCI Data Security Standard: Self-Assessment Questionnaire C-VT and Attestation	Eligible Merchants[9]
PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation	Eligible Merchants[9]
PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation	Eligible Merchants and service providers[9]
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	All merchants and service providers

[9] 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."