



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

---

**Understanding the Intent of the Requirements**

**Version 1.1**

February 2008

## Table of Contents

---

<b>Cardholder Data and Sensitive Authentication Data Elements.....</b>	<b>iii</b>
<i>Location of Cardholder data and Sensitive Authentication Data.....</i>	<i>iv</i>
<i>Track 1 vs. Track 2 Data .....</i>	<i>v</i>
<b>Related Guidance for the PCI Data Security Standard.....</b>	<b>Error! Bookmark not defined.</b>
<b>Guidance for Requirements 1 and 2: Build and Maintain a Secure Network .....</b>	<b>2</b>
<i>Requirement 1: Install and maintain a firewall configuration to protect cardholder data.....</i>	<i>2</i>
<i>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.....</i>	<i>7</i>
<b>Guidance for Requirements 3 and 4: Protect Cardholder Data .....</b>	<b>10</b>
<i>Requirement 3: Protect stored cardholder data .....</i>	<i>10</i>
<i>Requirement 4: Encrypt transmission of cardholder data across open, public networks.....</i>	<i>15</i>
<b>Guidance for Requirements 5 and 6: Maintain a Vulnerability Management Program.....</b>	<b>16</b>
<i>Requirement 5: Use and regularly update anti-virus software or programs.....</i>	<i>16</i>
<i>Requirement 6: Develop and maintain secure systems and applications.....</i>	<i>17</i>
<b>Guidance for Requirements 7, 8, and 9: Implement Strong Access Control Measures .....</b>	<b>21</b>
<i>Requirement 7: Restrict access to cardholder data by business need-to-know .....</i>	<i>21</i>
<i>Requirement 8: Assign a unique ID to each person with computer access.....</i>	<i>22</i>
<i>Requirement 9: Restrict physical access to cardholder data .....</i>	<i>25</i>
<b>Guidance for Requirements 10 and 11: Regularly Monitor and Test Networks.....</b>	<b>28</b>
<i>Requirement 10: Track and monitor all access to network resources and cardholder data .....</i>	<i>28</i>
<i>Requirement 11: Regularly test security systems and processes.....</i>	<i>31</i>
<b>Guidance for Requirement 12: Maintain an Information Security Policy .....</b>	<b>33</b>
<i>Requirement 12: Maintain a policy that addresses information security for employees and contractors .....</i>	<i>33</i>
<b>Guidance for Requirement A.1: PCI DSS Applicability for Hosting Providers .....</b>	<b>38</b>
<b>Appendix A: PCI Data Security Standard: Related Documents.....</b>	<b>39</b>

## Preface

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

**NOTE: *Navigating PCI DSS: Understanding the Intent of the Requirements* is for guidance only. When completing a PCI DSS on-site assessment or Self Assessment Questionnaire (SAQ), the PCI DSS v 1.1, the PCI DSS Security Audit Procedures, and the PCI DSS Self-Assessment Questionnaires v1.1 are the documents of record.**

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

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

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

## Cardholder Data and Sensitive Authentication Data Elements

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

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

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

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

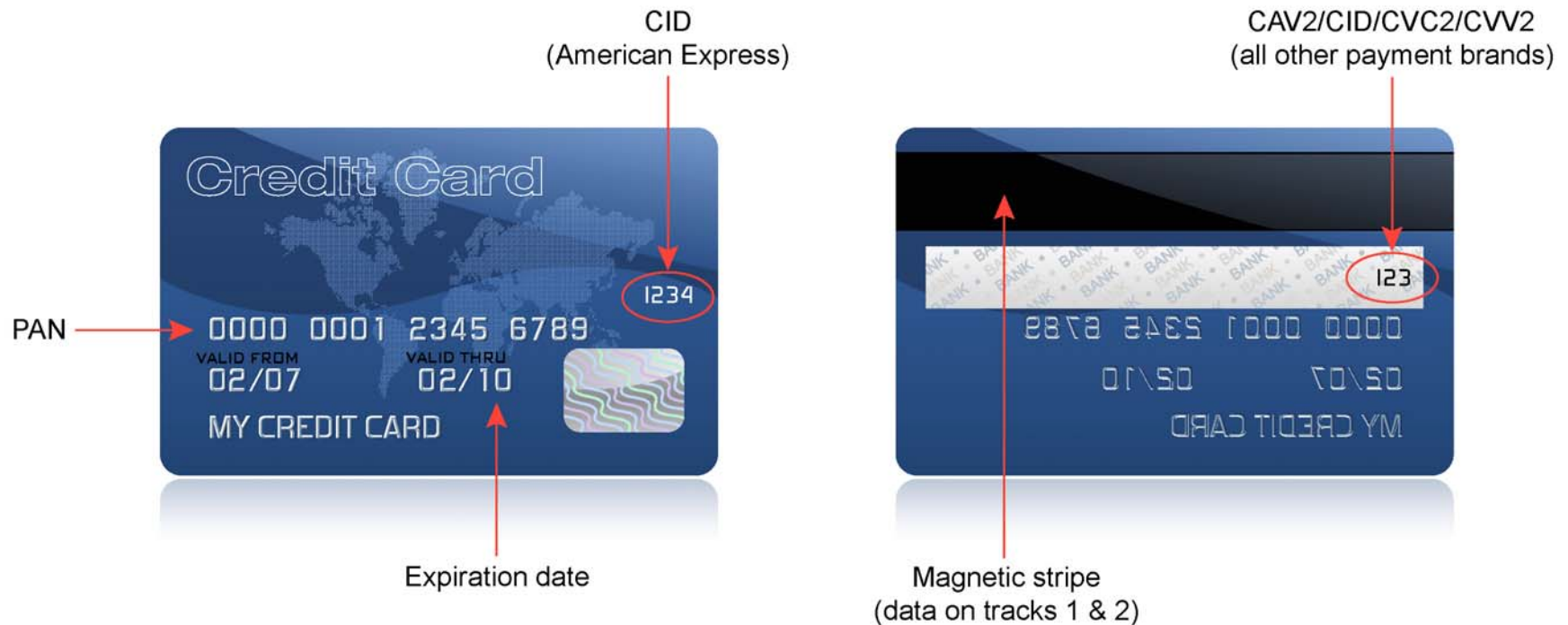
	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3, 4
<b>Cardholder Data</b>	Primary Account Number	Yes	Yes	Yes
	Cardholder Name <sup>1</sup>	Yes	Yes <sup>1</sup>	No
	Service Code <sup>1</sup>	Yes	Yes <sup>1</sup>	No
	Expiration Date <sup>1</sup>	Yes	Yes <sup>1</sup>	No
<b>Sensitive Authentication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

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

<sup>2</sup> *Do not store sensitive authentication data subsequent to authorization (not even if encrypted).*

## Location of Cardholder Data and Sensitive Authentication Data

Sensitive authentication data consists of magnetic stripe (or track) data<sup>3</sup>, card validation code or value<sup>4</sup>, and PIN data<sup>5</sup>. **Storage of sensitive authentication data is prohibited!** This data is very valuable to hackers as it allows them to generate fake payment cards and create fraudulent transactions. See *PCI DSS Glossary, 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.



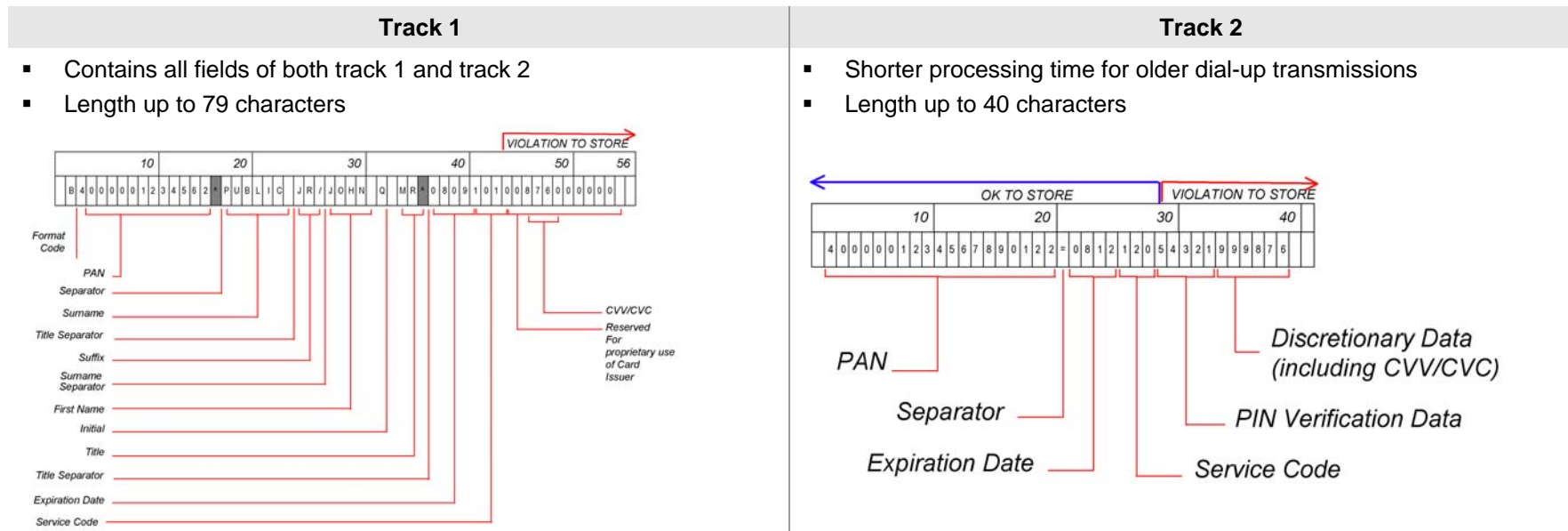
<sup>3</sup> Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data subsequent to transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

<sup>4</sup> 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.

<sup>5</sup> 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) data is stored, hackers 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.



## Related Guidance for the PCI Data Security Standard

### Build and Maintain a Secure Network

---

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

### Protect Cardholder Data

---

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

### Maintain a Vulnerability Management Program

---

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

### Implement Strong Access Control Measures

---

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

### Regularly Monitor and Test Networks

---

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

### Maintain an Information Security Policy

---

- Requirement 12: Maintain a policy that addresses information security

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

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

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal 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 the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Requirement	Guidance
<b>1.1</b> Establish firewall configuration standards that include the following:	Firewalls are software or hardware devices that block unwanted entry into the network. Without policies and procedures in place to document how staff should configure firewalls, a business could easily lose its first line of defense in data-protection.
<b>1.1.1</b> A formal process for approving and testing all external network connections and changes to the firewall configuration	A policy and process for approving and testing all connections and changes to the firewall will help prevent security problems caused by misconfiguration of the network or firewall.
<b>1.1.2</b> A 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. Without a network diagram, devices may be overlooked and may unknowingly become un-protected and thus vulnerable to compromise.
<b>1.1.3</b> 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 hacker's obtaining access to the internal network.
<b>1.1.4</b> 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.

Requirement	Guidance
<b>1.1.5</b> Documented list of services and ports necessary for business	Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities—and many organizations do not patch security vulnerabilities for services and ports they don't use (even though the vulnerabilities are still present). Each organization should clearly decide which services and ports are necessary for their business, document them for their records, and ensure that all other services and ports are disabled or removed. Also, organizations should consider blocking all traffic and only re-open those ports once a need has been determined and documented.
<b>1.1.6</b> Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	
<b>1.1.7</b> Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	
<b>1.1.8</b> Quarterly review of firewall and router rule sets	This review gives the organization a quarterly opportunity to clean up any unneeded, outdated, or incorrect rules, and ensures that all rule sets allow only authorized service and ports that match business justifications.
<b>1.1.9</b> Configuration standards for routers.	These devices, along with firewalls, are part of the architecture that controls the entry points into the network. Documented policies help staff to configure and secure routers, and ensure that the organization's first line of defense in the protection of its data remains strong.
<b>1.2</b> Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	If a firewall is installed but does not have rules that control or limit certain traffic, malicious users may still be able to exploit vulnerable protocols and ports to attack your network.
<b>1.3</b> Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:	

Requirement	Guidance
<p><b>1.3.1</b> Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)</p>	<p>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 hackers.</p>
<p><b>1.3.2</b> Not allowing internal addresses to pass from the Internet into the DMZ</p>	<p>For example, hackers 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 hacker is inside your network, they can begin to compromise your systems.</p> <p>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.</p> <p>For more information on packet filtering, consider obtaining information on a corollary technique called “egress filtering.”</p>
<p><b>1.3.3</b> Implementing stateful inspection, also known as dynamic packet filtering (that is, only “established” connections are allowed into the network)</p>	<p>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 someone trying to spoof or trick the firewall into allowing the connection.</p>
<p><b>1.3.4</b> Placing the database in an internal network zone, segregated from the DMZ</p>	<p>Payment card account information requires the highest level of information protection. If account information is located within the DMZ, access to this information is easier for an external attacker, since there are fewer layers to penetrate. Without a firewall protecting account information, that data is vulnerable to malicious users from inside a flat network and any hackers that are able to penetrate from outside the network.</p>
<p><b>1.3.5</b> Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment</p>	<p>This requirement is intended to prevent hackers from accessing the organization's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an external server).</p>
<p><b>1.3.6</b> Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration</p>	<p>While running configuration files are usually implemented with secure settings, the start-up file (routers only run these files upon re-start) may not be implemented with the same secure settings because they only run occasionally. When a router does re-start without the same secure settings as those in the running configuration files, it may result in weaker rules that allow a hacker into the network.</p>

Requirement	Guidance
<p><b>1.3.7</b> Denying all other inbound and outbound traffic not specifically allowed</p>	<p>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.</p>
<p><b>1.3.8</b> Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)</p>	<p>The known (or unknown) implementation and exploitation of wireless technology within a network is a common path 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, a hacker could easily and "invisibly" enter the network. If firewalls do not restrict access from wireless networks into the payment card environment, hackers that gain unauthorized access to the wireless network can easily connect to the payment card environment and compromise account information.</p>
<p><b>1.3.9</b> Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network</p>	<p>If a computer does not have a firewall or anti-virus program installed, spyware, Trojans, viruses, and worms (malware) may be downloaded 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.</p>
<p><b>1.4</b> Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).</p>	<p>A firewall's intent is to manage and control all connections between public systems and internal systems (especially those that store cardholder data). If direct access is allowed between public systems and those that store cardholder data, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.</p>
<p><b>1.4.1</b> Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic.</p>	<p>The DMZ is the part of the firewall that faces the public Internet and manages connections between the Internet and internal services that an organization needs to have available to the public (like a web server). It is the first line of defense in isolating and separating traffic that needs to communicate with the internal network from traffic that does not.</p>
<p><b>1.4.2</b> Restrict outbound traffic from payment card applications to IP addresses within the DMZ.</p>	<p>The DMZ also should evaluate all traffic outbound from inside the network to ensure that all outbound traffic follows established rules. For the DMZ to serve this function effectively, connections from inside the network to any addresses outside the network should not be allowed unless they first go through and are evaluated for legitimacy by the DMZ.</p>

Requirement	Guidance
<b>1.5</b> Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	IP masquerading, which is managed by the firewall, allows an organization to have internal addresses that are only visible inside the network and external address that are visible externally. If a firewall does not “hide” or mask the IP addresses of the internal network, a hacker could discover internal IP addresses and attempt to access the network with a spoofed IP address.

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

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

Requirement	Guidance
<p><b>2.1</b> Always change vendor-supplied defaults <b>before</b> installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).</p>	<p>Hackers (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.</p>
<p><b>2.1.1</b> <b>For wireless environments</b>, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.</p>	<p>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.</p>
<p><b>2.2</b> 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 as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).</p>	<p>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.</p>

Requirement	Guidance
<p><b>2.2.1</b> Implement only one primary function per server (<i>for example, web servers, database servers, and DNS should be implemented on separate servers</i>)</p>	<p>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:</p> <ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol> <p>This requirement is meant for servers (usually Unix, Linux, or Windows based), but not mainframe systems.</p>
<p><b>2.2.2</b> Disable all unnecessary and insecure services and protocols (<i>services and protocols not directly needed to perform the devices' specified function</i>)</p>	<p>As stated at 1.1.7, there are many protocols that a business may need (or have enabled by default) that are commonly used by hackers to compromise a network. To ensure that these services and protocols are always disabled when new servers are deployed, this requirement should be part of your organization's configuration standards and related processes.</p>
<p><b>2.2.3</b> Configure system security parameters to prevent misuse</p>	<p>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.</p>
<p><b>2.2.4</b> Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.</p>	<p>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).</p>
<p><b>2.3</b> Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.</p>	<p>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 hacker could use this information to access the network, become administrator, and steal data.</p>

Requirement	Guidance
<b>2.4</b> Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in the PCI DSS – see “ <i>Appendix A: PCI DSS Applicability for Hosting Providers.</i> ”	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 hacker to compromise one client's data and thereby gain access to all other clients' data. See also the guidance in this document at “ <i>Guidance for Requirement A.1.</i> ”

## Guidance for Requirements 3 and 4: Protect Cardholder Data

### Requirement 3: Protect stored cardholder data

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

Requirement	Guidance
<p><b>3.1</b> Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.</p>	<p>Extended storage of cardholder data that exceeds business need creates an unnecessary risk. The only cardholder data that may be stored is the primary account number or PAN (rendered unreadable), expiry date, name, and service code. <b>Remember, if you don't need it, don't store it!</b></p>
<p><b>3.2</b> Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following requirements, 3.2.1 through 3.2.3:</p>	<p>Sensitive authentication data consists of magnetic stripe (or track) data<sup>6</sup>, card validation code or value<sup>7</sup>, and PIN data<sup>8</sup>. <b>Storage of sensitive authentication data is prohibited!</b> This data is very valuable to hackers as it allows them to generate fake payment cards and create fraudulent transactions. See <i>PCI DSS Glossary, Abbreviations, and Acronyms</i> for the full definition of "sensitive authentication data."</p>

<sup>6</sup> Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data subsequent to transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

<sup>7</sup> 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.

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

Requirement	Guidance
<p><b>3.2.1</b> Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data</p> <p><i>In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i></p> <p><i>Note: See PCI DSS Glossary, Abbreviations, and Acronyms for additional information.</i></p> <p><b>3.2.2</b> Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions</p> <p><i>Note: See PCI DSS Glossary, Abbreviations, and Acronyms for additional information.</i></p>	<p>If full track data is stored, hackers 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.</p> <p>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, hackers can execute fraudulent Internet and MO/TO transactions. This storage also violates payment brands' regulations and can lead to fines and penalties.</p>
<p><b>3.2.3</b> Do not store the personal identification number (PIN) or the encrypted PIN block.</p>	<p>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, hackers can execute fraudulent PIN-based debit transactions (e.g., ATM withdrawals). Such storage also violates payment brands' regulations and can lead to fines and penalties.</p>

Requirement	Guidance
<p><b>3.3</b> Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).</p> <p><i>Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).</i></p>	<p>The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data's being obtained by unauthorized individuals and used fraudulently. Note that this data can be displayed in full form on the "merchant copy" receipts, or for those with a specific need to see the full PAN.</p>
<p><b>3.4</b> Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:</p>	<p>Lack of protection of PANs can allow unauthorized internal users and intruders to view or download this data. PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. Damage from theft or loss of backup tapes during transport can be reduced by ensuring PANs are rendered unreadable via encryption, truncation, or hashing. Since audit, troubleshooting, and exception logs have to be retained, you can prevent disclosure of data in logs by rendering PANs unreadable (or removing or masking them) in logs.</p>
<ul style="list-style-type: none"> <li>• Strong one-way hash functions (hashed indexes)</li> <li>• Truncation</li> </ul>	<p>One-way hash functions such as SHA-1 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).</p> <p>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.).</p>
<ul style="list-style-type: none"> <li>• Index tokens and pads (pads must be securely stored)</li> </ul>	<p>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.</p>
<ul style="list-style-type: none"> <li>• Strong cryptography with associated key management processes and procedures.</li> </ul>	<p>The intent of strong cryptography (see definition and key lengths in the <i>PCI DSS Glossary, Abbreviations, and Acronyms</i>) is that the encryption be based</p>

Requirement	Guidance
<p><b>The MINIMUM account information that must be rendered unreadable is the PAN.</b></p> <p><i>If for some reason, a company is unable to encrypt cardholder data, refer to "Appendix B: Compensating Controls." the PCI DSS.</i></p>	<p>on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm).</p>
<p><b>3.4.1</b> 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 system or Active Directory accounts). Decryption keys must not be tied to user accounts.</p>	<p>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:</p> <ol style="list-style-type: none"> <li>1) A direct association with the operating system, or</li> <li>2) Decryption keys that are associated with user accounts.</li> </ol>
<p><b>3.5</b> Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.</p>	<p>Encryption keys must be strongly protected because those who obtain access will be able to decrypt data.</p>
<p><b>3.5.1</b> Restrict access to keys to the fewest number of custodians necessary</p>	<p>There should be very few who have access to encryption keys, usually only those who have key custodian responsibilities.</p>
<p><b>3.5.2</b> Store keys securely in the fewest possible locations and forms.</p>	<p>Encryption keys must be stored securely, usually encrypted with key-encrypting keys, and stored in very few locations.</p>
<p><b>3.6</b> Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:</p>	<p>The manner in which encryption keys are managed is a critical part of the continued security of the encryption solution. A good key management process, whether it is manual or automated as part of the encryption product, addresses all key elements at 3.6.1 through 3.6.10.</p>
<p><b>3.6.1</b> Generation of strong keys</p>	<p>The encryption solution must generate strong keys, as defined in the <i>PCI DSS Glossary, Abbreviations, and Acronyms</i> under "strong cryptography."</p>
<p><b>3.6.2</b> Secure key distribution</p>	<p>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.</p>
<p><b>3.6.3</b> Secure key storage</p>	<p>The encryption solution must store keys securely, meaning the keys are not stored in the clear (encrypt them with a key-encryption key).</p>

Requirement	Guidance
<p><b>3.6.4</b> Periodic changing of keys</p> <ul style="list-style-type: none"> <li>As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically.</li> <li>At least annually.</li> </ul>	<p>If provided by encryption application vendor, follow any vendor processes or recommendations for periodic changing of keys.</p> <p>Annual changing of encryption keys is imperative to minimize the risk of someone's obtaining the encryption keys, and being able to decrypt data.</p>
<p><b>3.6.5</b> Destruction of old keys</p>	<p>Old keys that are no longer used or needed should be destroyed. If old keys need to be kept (to support archived, encrypted data, for example) they should be strongly protected. (See 3.6.6 below.)</p>
<p><b>3.6.6</b> Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)</p>	<p>Split knowledge and dual control of keys are used to eliminate the possibility of one person's having access to the whole key. This control is usually applicable for manual key-encryption systems, or where key management is not implemented by the encryption product. This type of control is usually implemented within hardware security modules.</p>
<p><b>3.6.7</b> Prevention of unauthorized substitution of keys</p>	<p>The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.</p>
<p><b>3.6.8</b> Replacement of known or suspected compromised keys</p>	<p>The encryption solution should allow for and facilitate a process to replace keys that are known to be, or suspected of being, compromised.</p>
<p><b>3.6.9</b> Revocation of old or invalid keys</p>	<p>This will ensure the keys can no longer be used.</p>
<p><b>3.6.10</b> Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.</p>	<p>This process will ensure the individual commits to the key-custodian role and understands its responsibilities.</p>

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

*Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.*

Requirement	Guidance
<p><b>4.1</b> Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.</p> <p><i>Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).</i></p>	<p>Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a hacker to intercept and/or divert data while in transit. Note that SSL versions prior to v3.0 contain documented vulnerabilities, such as buffer overflows, that an attacker can use to gain control of the affected system.</p>
<p><b>4.1.1 For wireless networks transmitting cardholder data</b>, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:</p> <ul style="list-style-type: none"> <li>• Use with a minimum 104-bit encryption key and 24 bit-initialization value</li> <li>• Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS</li> <li>• Rotate shared WEP keys quarterly (or automatically if the technology permits)</li> <li>• Rotate shared WEP keys whenever there are changes in personnel with access to keys</li> <li>• Restrict access based on media access code (MAC) address.</li> </ul>	<p>Hackers use free and widely available tools to eavesdrop on wireless communications. Use of appropriate encryption can prevent eavesdropping and disclosure of sensitive information across the network. Many known compromises of cardholder data stored only in the wired network originated when a hacker expanded access from a wireless network. WEP encryption should never be used alone since it is vulnerable due to weak initial vectors (IV) in the WEP key-exchange process, and lack of required rotation of keys. An attacker can use freely available brute-force cracking tools to penetrate WEP encryption.</p>
<p><b>4.2</b> Never send unencrypted PANs by e-mail.</p>	<p>E-mail can be easily intercepted by packet-sniffing during delivery traversal across internal and public networks.</p>

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

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

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

Requirement	Guidance
<p><b>5.1</b> Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers)</p> <p><i>Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.</i></p>	<p>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 viruses can attack and disable your network.</p>
<p><b>5.1.1</b> Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.</p>	<p>It is important to protect against <b>ALL</b> types and forms of malicious software.</p>
<p><b>5.2</b> Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.</p>	<p>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.</p>

## 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. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. 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
<p><b>6.1</b> Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.</p>	<p>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 systems as soon as possible, a hacker 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 receive a lower priority.</p>
<p><b>6.2</b> Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.</p>	<p>The intention of this requirement is that organizations are kept up-to-date with new vulnerabilities so they can appropriately protect their network, and incorporate newly discovered and relevant vulnerabilities into their configuration standards.</p>
<p><b>6.3</b> Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.</p>	<p>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.</p>
<p><b>6.3.1</b> Testing of all security patches and system and software configuration changes before deployment</p>	<p>Ensure all installations and changes are performing as expected, and that they do not have any functions that are unexpected, unwanted, or harmful.</p>
<p><b>6.3.2</b> Separate development, test, and production environments</p>	<p>Often development and test environments are less secure than the production environment. Without adequate separation, the production environment and cardholder data may be at risk due to vulnerabilities or weak internal processes.</p>
<p><b>6.3.3</b> Separation of duties between development, test, and production environments</p>	<p>This minimizes the number of personnel with access to the production environment and cardholder data, and helps ensure that access is limited to those who truly need that access.</p>

Requirement	Guidance
<b>6.3.4</b> 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 allows potential hackers, as well as developers, the opportunity to gain unauthorized access to production information.
<b>6.3.5</b> 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.
<b>6.3.6</b> Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers	Custom application accounts, usernames, and passwords should be removed from production code before the application becomes active or are released to customers, since these items may give away information about the functioning of the application. Possession of such information could facilitate compromise of the application and related cardholder data.
<b>6.3.7</b> Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	Security vulnerabilities in custom code are commonly exploited by hackers to gain access to a network and compromise cardholder data. Those with knowledge of secure coding techniques should review code to identify vulnerabilities.
<b>6.4</b> Follow change control procedures for all system and software configuration changes. The procedures must include the following:	Without proper software change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced. If related personnel policies for background checks and system access controls are not adequate, there is a risk that untrustworthy and untrained individuals may have unrestricted access to software code, terminated employees may have the opportunity to compromise systems, and unauthorized actions may not be detected.
<b>6.4.1</b> 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.
<b>6.4.2</b> Management sign-off by appropriate parties	Management approval indicates that the change is a legitimate and authorized one sanctioned by the organization.
<b>6.4.3</b> Testing of operational functionality	Thorough testing should be performed to verify that all actions are expected, reports are accurate, that all possible error conditions react properly, etc.
<b>6.4.4</b> 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
<p><b>6.5</b> Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:</p>	<p>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.</p>
<p><b>6.5.1</b> Unvalidated input</p>	<p>Information from web requests should be validated before being sent to the web application—for example, checks for all alpha characters, mix of alpha and numeric, etc., should be done. Without these checks, hackers can pass invalid information into an application and attack components inside the network through the application.</p>
<p><b>6.5.2</b> Broken access control (for example, malicious use of user IDs)</p>	<p>Malicious users often attempt to scan and enumerate existing user accounts on applications in order to find an attack entry point. Once an existing account is found, an attacker will try to use default passwords or brute force to access the application.</p>
<p><b>6.5.3</b> Broken authentication and session management (use of account credentials and session cookies)</p>	<p>Account credentials and session tokens should be properly protected. Attacks on passwords, keys, session cookies, or other tokens can defeat authentication restrictions and allow hackers to assume other users' identities. Additionally, cookies may store cardholder information and are by default stored in clear text.</p>
<p><b>6.5.4</b> Cross-site scripting (XSS) attacks</p>	<p>With these attacks, a web application is used to send an attack to an end user's browser and can result in disclosure of the end user's session token, an attack on the end user's machine, and a hacker's sending spoofed content to fool the user.</p>
<p><b>6.5.5</b> Buffer overflows</p>	<p>Hackers can crash web application components that do not properly validate input (see also 6.5.1 above), and may be able to take control of processes on the related server.</p>
<p><b>6.5.6</b> Injection flaws (for example, structured query language (SQL) injection)</p>	<p>To speed up connectivity and reduce performance at the server end, client-side validation of input and manipulation of data is often required. It is often a relatively trivial exercise for hackers to bypass this checking and use the web application to send malicious commands to the server to initiate attacks such as buffer overflows, or to reveal both confidential information and server application functionality. This is also a popular means of conducting fraudulent transactions on commerce-enabled sites.</p>

Requirement	Guidance
<p><b>6.5.7</b> Improper error handling</p>	<p>Often, incorrect error handling provides information that helps a hacker compromise the system. If a hacker can create errors that the web application does not handle properly, they can gain detailed system information, create denial-of-service interruptions, cause security to fail, or crash the server. For example, the message "incorrect password provided" tells them the username provided was accurate and that they should focus their efforts only on the password.</p> <p><i>Use more generic error messages, like "data could not be verified."</i></p>
<p><b>6.5.8</b> Insecure storage</p>	<p>This relates to insecure use of cryptography. Since cryptography applications are difficult to code properly, this frequently results in weak protection of stored data and cryptography that is easier to break.</p>
<p><b>6.5.9</b> Denial of service</p>	<p>Hackers can consume web application resources to the point that other users can no longer use the application. Hackers can also lock users out of their accounts or cause the application to fail.</p>
<p><b>6.5.10</b> Insecure configuration management</p>	<p>Having a strong server configuration standard is critical to having secure web applications. Servers have many configuration options to control security and are not secure out of the box.</p>
<p><b>6.6</b> Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:</p> <ul style="list-style-type: none"> <li>• Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security</li> <li>• Installing an application layer firewall in front of web-facing applications.</li> </ul> <p><i>Note: 6.6 is considered a best practice until June 30, 2008, after which it becomes a requirement.</i></p>	<p>Attacks on web-facing applications are common and often successful, and are allowed by poor coding practices. This requirement for application code reviews or application-layer firewalls is intended to greatly reduce the number of compromises on web-facing applications that result in breaches of cardholder data.</p> <p>A tool that performs code reviews and/or scans for application vulnerabilities can also be used to satisfy this requirement.</p> <p>Application firewalls are used to filter and block non-essential traffic at the application layer. Used in conjunction with a network based firewall, a properly configured application layer firewall prevents application layer attacks should applications be improperly coded or configured.</p>

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

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

*This requirement ensures critical data can only be accessed by authorized personnel.*

Requirement	Guidance
<p><b>7.1</b> Limit access to computing resources and cardholder information only to those individuals whose job requires such access.</p>	<p>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. Your organization should create a clear policy for data access control to define how, and to whom, access is granted.</p>
<p><b>7.2</b> Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.</p>	<p>Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data.</p>

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

*Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.*

Requirement	Guidance
<p><b>8.1</b> Identify all users with a unique user name before allowing them to access system components or cardholder data.</p>	<p>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.</p>
<p><b>8.2</b> In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> <li>• Password</li> <li>• Token devices (e.g., SecureID, certificates, or public key)</li> <li>• Biometrics.</li> </ul>	<p>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).</p>
<p><b>8.3</b> Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.</p>	<p>Two-factor authentication technologies provide a one-time password, to be used when an additional authentication item is needed for higher-risk accesses, like 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)).</p>
<p><b>8.4</b> Encrypt all passwords during transmission and storage on all system components.</p>	<p>Many network devices and applications transmit the user ID and unencrypted password across the network and/or also store the passwords without encryption. A hacker can easily intercept the encrypted 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.</p>
<p><b>8.5</b> Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:</p>	<p>Since one of the first steps a hacker will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for user authentication and password management.</p>

Requirement	Guidance
<b>8.5.1</b> 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.
<b>8.5.2</b> Verify user identity before performing password resets.	Many hackers 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.
<b>8.5.3</b> Set first-time passwords to a unique value for each user and change immediately after the first use.	If the same password is used for every new user set up, an internal user, former employee, or hacker may know or easily discover this password, and use it to gain access to accounts.
<b>8.5.4</b> Immediately revoke access for any terminated users.	If an employee has left the company, and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur. This access could happen from the former employee or from a malicious user who exploits the older and/or unused account. Consider implementing a process with HR for immediate notification when an employee is terminated so that the user account can be quickly revoked.
<b>8.5.5</b> Remove 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.
<b>8.5.6</b> Enable accounts used by vendors for remote maintenance only during the time period needed.	Allowing vendors (like POS vendors) to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor’s environment or from a hacker who finds and uses this always-ready external entry point into your network. Please also see 12.3.8 and 12.3.9 for more on this topic.
<b>8.5.7</b> Communicate password procedures and policies to all users who have access to cardholder data.	Communicating password procedures to all users helps those users understand and abide by the policies, and to be alert for any malicious users 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”).
<b>8.5.8</b> Do not use group, shared, or generic accounts and passwords.	If multiple users share the same account and password, it becomes impossible to assign accountability for, or to have effective logging of, an individual’s actions, since a given action could have been performed by anyone in the group that shares the account and password.

Requirement	Guidance
<b>8.5.9</b> Change user passwords at least every 90 days.	<p>Strong passwords are the first line of defense into a network since a hacker will often first try to find accounts with weak or non-existent passwords. There is more time for an attacker 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.</p>
<b>8.5.10</b> Require a minimum password length of at least seven characters.	
<b>8.5.11</b> Use passwords containing both numeric and alphabetic characters.	
<b>8.5.12</b> 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.	
<b>8.5.13</b> Limit repeated access attempts by locking out the user ID after not more than six attempts.	<p>Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (password cracking), until they achieve success and gain access to a user's account.</p>
<b>8.5.14</b> Set the lockout duration to thirty minutes or until administrator enables the user ID.	<p>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 hacker from continually guessing the password (they will have to stop for at least 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.</p>
<b>8.5.15</b> If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	<p>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.</p>
<b>8.5.16</b> Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	<p>Without database authentication, potential for unauthorized or malicious access to the database increases, and such access cannot be logged since the user has not authenticated and is therefore not known to the system. Also, database access should be always through programmed 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).</p>

**Requirement 9: Restrict physical access to cardholder data**

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

Requirement	Guidance
<p><b>9.1</b> Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.</p>	<p>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.</p>
<p><b>9.1.1</b> Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law</p>	<p>Without “eyes” on critical systems, physical breaches are harder to prevent and investigate, and the attackers cannot be identified.</p>
<p><b>9.1.2</b> Restrict physical access to publicly accessible network jacks</p>	<p>Restricting access to network jacks will prevent hackers 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.</p>
<p><b>9.1.3</b> Restrict physical access to wireless access points, gateways, and handheld devices.</p>	<p>Without security over access to wireless components and devices, malicious users could use your company’s unattended wireless devices to access your network resources, or even connect their own devices to your wireless network, giving them unauthorized access. Consider placing wireless access points and gateways in secure storage areas, such as within locked closets. Ensure strong encryption is enabled. Enable automatic device lockout on wireless handheld devices after a period of inactivity, and set your devices to require a password when powering on.</p>

Requirement	Guidance
<p><b>9.2</b> Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.</p> <p><i>“Employee” refers to full-time and part-time employees, temporary employees and personnel, and consultants who are “resident” on the entity’s site. A “visitor” is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.</i></p>	<p>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.</p>
<p><b>9.3</b> Make sure all visitors are handled as follows:</p> <p><b>9.3.1</b> Authorized before entering areas where cardholder data is processed or maintained.</p> <p><b>9.3.2</b> Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees.</p> <p><b>9.3.3</b> Asked to surrender the physical token before leaving the facility or at the date of expiration.</p>	<p>Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to your facilities (and potentially, to cardholder data).</p> <p>Visitor controls are important to ensure visitors only enter areas they are authorized to enter, that they are identifiable as visitors so employees can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.</p>
<p><b>9.4</b> Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.</p>	<p>A visitor log is cheap and easy 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.</p>
<p><b>9.5</b> Store media backups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.</p>	<p>Backups may contain cardholder data and, if stored in a non-secured facility, 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.</p>
<p><b>9.6</b> Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.</p>	<p>Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on portable media, printed out, or left on someone’s desk. Consider procedures and processes for protecting cardholder data on media distributed to internal or external users. Without such procedures data can be lost or stolen and used for fraudulent purposes.</p>

Requirement	Guidance
<b>9.7</b> Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:	
<b>9.7.1</b> Classify the media so it can be identified as confidential.	Media not identified as confidential may not be treated with the care it requires and may be lost or stolen. Include a media classification process in the procedures recommended in 9.6 above.
<b>9.7.2</b> 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. Contract with 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.
<b>9.8</b> 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. Include development of a management-approved process for moving media in the procedures recommended in 9.6 above.
<b>9.9</b> Maintain strict control over the storage and accessibility of media that contains cardholder data.	Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time. Include development of a process to limit access to media with cardholder data in the procedures recommended above at 9.6.
<b>9.9.1</b> Properly inventory all media and make sure it is securely stored.	If media is not inventoried, stolen or lost media may not be noticed for a long time. Include development of a process for media inventories and secure storage in the procedures recommended above at 9.6.
<b>9.10</b> Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:	If steps are not taken to destroy information contained on PC hard disks and CDs, and on paper, disposal of such information may result in compromise and lead to financial or reputation loss. For example, hackers may use a technique known as “dumpster diving,” where they search through trashcans and recycle bins, and use found information to launch an attack. Include development of a process for properly destroying media with cardholder data, including proper storage of such media prior to destruction, in the procedures recommended above at 9.6
<b>9.10.1</b> Cross-cut shred, incinerate, or pulp hardcopy materials	
<b>9.10.2</b> Purge, degauss, shred, or otherwise destroy electronic media 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. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.*

Requirement	Guidance
<p><b>10.1</b> Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.</p>	<p>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.</p>
<p><b>10.2</b> Implement automated audit trails for all system components to reconstruct the following events:</p> <ul style="list-style-type: none"> <li><b>10.2.1</b> All individual user accesses to cardholder data</li> <li><b>10.2.2</b> All actions taken by any individual with root or administrative privileges</li> <li><b>10.2.3</b> Access to all audit trails</li> <li><b>10.2.4</b> Invalid logical access attempts</li> <li><b>10.2.5</b> Use of identification and authentication mechanisms</li> <li><b>10.2.6</b> Initialization of the audit logs</li> <li><b>10.2.7</b> Creation and deletion of system-level objects.</li> </ul>	<p>Hackers on the network will often perform multiple access attempts on targeted systems. Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up.</p>

Requirement	Guidance
<p><b>10.3</b> Record at least the following audit trail entries for all system components for each event:</p> <ul style="list-style-type: none"> <li><b>10.3.1</b> User identification</li> <li><b>10.3.2</b> Type of event</li> <li><b>10.3.3</b> Date and time</li> <li><b>10.3.4</b> Success or failure indication</li> <li><b>10.3.5</b> Origination of event</li> <li><b>10.3.6</b> Identity or name of affected data, system component, or resource.</li> </ul>	<p>By recording these entries for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, where, and how.</p>
<p><b>10.4</b> Synchronize all critical system clocks and times.</p>	<p>If a hacker has entered the network, they will often attempt to change the time stamps of their actions within the audit logs to prevent detection of their activity. For post-incident forensics teams, the time of each activity is critical in determining how the systems were compromised. A hacker may also try to directly change the clock on a time server, if access restrictions are not appropriate, to restate the time to before the hacker was in the network.</p>
<p><b>10.5</b> Secure audit trails so they cannot be altered.</p>	<p>Often a hacker 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.</p>
<ul style="list-style-type: none"> <li><b>10.5.1</b> Limit viewing of audit trails to those with a job-related need</li> <li><b>10.5.2</b> Protect audit trail files from unauthorized modifications</li> <li><b>10.5.3</b> Promptly back up audit trail files to a centralized log server or media that is difficult to alter</li> <li><b>10.5.4</b> Copy logs for wireless networks onto a log server on the internal LAN.</li> </ul>	<p>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).</p>

Requirement	Guidance
<p><b>10.5.5</b> Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).</p>	<p>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 hacker has tampered with a log file. There are both off-the-shelf and open source tools available for file integrity monitoring.</p>
<p><b>10.6</b> 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).</p> <p><i>Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.</i></p>	<p>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.</p>
<p><b>10.7</b> Retain audit trail history for at least one year, with a minimum of three months online availability.</p>	<p>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.</p>

**Requirement 11: Regularly test security systems and processes**

*Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.*

Requirement	Guidance
<p><b>11.1</b> (a) Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.</p>	<p>If not tested consistently, gaps will occur in security controls that can be exploited.</p>
<p>(b) Use a wireless analyzer at least quarterly to identify all wireless devices in use.</p>	<p>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 a hacker to easily and “invisibly” enter the network. In addition to wireless analyzers, “nmap” and other network tools that detect wireless devices can be used.</p>
<p><b>11.2</b> 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).</p> <p><i>Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company’s internal staff.</i></p>	<p>A vulnerability scan is an automated tool run against external and internal network access points and devices and servers on the network, to expose potential vulnerabilities and identify ports in networks that could be found and exploited by hackers. Once these weaknesses are identified, the entity corrects them to make their network more secure.</p>
<p><b>11.3</b> Perform 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:</p> <ul style="list-style-type: none"> <li><b>11.3.1</b> Network-layer penetration tests</li> <li><b>11.3.2</b> Application-layer penetration tests.</li> </ul>	<p>Network and application penetration tests are different from vulnerability scans in that penetration tests are more manual, attempt to actually exploit some of the vulnerabilities identified in scans, and follow practices used by hackers to take advantage of weak security systems or processes.</p> <p>Before applications, network devices, and systems are released into production, they should be hardened and secured using security best practices (per requirement 2.2). Vulnerability scans and penetration tests will expose any remaining vulnerabilities that could later be found and exploited by hackers.</p>

Requirement	Guidance
<p><b>11.4</b> (a) Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.</p> <p>(b) Keep all intrusion detection and prevention engines up-to-date.</p>	<p>These tools compare the traffic coming into the network with known “signatures” of thousands of compromise types (hacker tools, Trojans, etc.), 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.</p> <p>There are thousands of compromise types, with more being discovered on a daily basis. Stale versions of these systems will not have current “signatures” and will not identify new vulnerabilities that could lead to an undetected breach. Vendors of these products provide frequent, often daily, updates.</p>
<p><b>11.5</b> Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.</p> <p><i>Critical files are not necessarily only those containing cardholder data. 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).</i></p>	<p>File integrity monitoring systems check for changes to critical files, and notify when such changes are noted. There are both off-the-shelf and open source tools available for file integrity monitoring. If not implemented and the output monitored, a hacker or user with malicious intent could alter file contents or steal data undetected.</p>

## Guidance for Requirement 12: Maintain an Information Security Policy

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

*A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.*

Requirement	Guidance
<p><b>12.1</b> Establish, publish, maintain, and disseminate a security policy that accomplishes the following:</p> <ul style="list-style-type: none"> <li><b>12.1.1</b> Addresses all requirements in this specification</li> <li><b>12.1.2</b> Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment</li> <li><b>12.1.3</b> Includes a review at least once a year and updates when the environment changes.</li> </ul>	<p>A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. A strong security policy sets the security tone for the whole company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.</p> <p>Security threats and protection methods evolve rapidly throughout the year. Without updating the security policy to reflect these changes, new protection measures to fight against these threats will not exist.</p>
<p><b>12.2</b> Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).</p>	<p>Daily operational security procedures act as “desk instructions” for workers to use in their day-to-day system administrative and maintenance activities. Undocumented operational security procedures will lead to workers who are not aware of the full scope of their tasks, processes that cannot be repeated easily by new workers, and potential gaps in these processes that may allow a hacker to gain access to critical systems and resources.</p>
<p><b>12.3</b> Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:</p>	<p>Employee usage policies can either prohibit use of such devices if that is company policy, or provide guidance for employees as to correct usage and implementation. If usage policies are not in place, employees may use devices in violation of company policy, may unknowingly set up modems and/or wireless networks with no security, and thereby allow hackers to gain access to critical systems and cardholder data. To ensure that company standards are followed and only approved technologies are implemented, consider confining implementation to operations teams only; do not let unspecialized/general employees install these technologies.</p>

Requirement	Guidance
<p><b>12.3.1</b> Explicit management approval</p>	<p>Without requiring proper management approval for implementation of these technologies, an employee may innocently implement a solution to a perceived business need, but also open a huge hole that subjects critical systems and data to hackers.</p>
<p><b>12.3.2</b> Authentication for use of the technology</p>	<p>If this technology is implemented without proper authentication (user IDs and passwords, tokens, VPNs, etc.), hackers may easily use this unprotected technology to access critical systems and cardholder data.</p>
<p><b>12.3.3</b> List of all such devices and personnel with access</p>	<p>Hackers may breach physical security and place their own devices on the network as a “back door.” Employees may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations. Consider establishing an official naming convention for devices, and label and log all devices in concert with established inventory controls.</p>
<p><b>12.3.4</b> Labeling of devices with owner, contact information, and purpose</p>	
<p><b>12.3.5</b> Acceptable uses of the technologies</p>	
<p><b>12.3.6</b> Acceptable network locations for the technologies</p>	<p>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 hacker to gain access to critical systems and cardholder data.</p>
<p><b>12.3.7</b> List of company-approved products</p>	
<p><b>12.3.8</b> Automatic disconnect of modem sessions after a specific period of inactivity</p>	<p>Modems are a frequent “back doors” to critical resources and cardholder data. By disconnecting modems when not in use (for example, those used to support your systems by your POS or other vendors), access and risk to networks is minimized. Consider using standard modem controls to disconnect devices after 15 minutes of inactivity. Please also see 8.5.6 for more on this topic.</p>
<p><b>12.3.9</b> Activation of modems for vendors only when needed by vendors, with immediate deactivation after use</p>	
<p><b>12.3.10</b> When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.</p>	<p>To ensure your employees are aware of their responsibilities to not store or copy cardholder data onto their local personal computer or other media, your company should have a policy that clearly prohibits such activities.</p>
<p><b>12.4</b> Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.</p>	<p>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.</p>

Requirement	Guidance
<p><b>12.5</b> Assign to an individual or team the following information security management responsibilities:</p> <ul style="list-style-type: none"> <li><b>12.5.1</b> Establish, document, and distribute security policies and procedures</li> <li><b>12.5.2</b> Monitor and analyze security alerts and information, and distribute to appropriate personnel</li> <li><b>12.5.3</b> Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations</li> <li><b>12.5.4</b> Administer user accounts, including additions, deletions, and modifications</li> <li><b>12.5.5</b> Monitor and control all access to data.</li> </ul>	<p>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.</p>
<p><b>12.6</b> Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.</p>	<p>If users are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through employee errors or intentional actions.</p>
<p><b>12.6.1</b> Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)</p>	<p>If the security awareness program does not include annual refresher sessions, key security processes and procedures may be forgotten or bypassed, resulting in exposed critical resources and cardholder data.</p>
<p><b>12.6.2</b> Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.</p>	<p>Requiring an employee signature helps ensure that they have read and understood the security policies/procedures, and that they have made a commitment to comply with these policies.</p>
<p><b>12.7</b> Screen potential employees to minimize the risk of attacks from internal sources.</p> <p><i>For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i></p>	<p>Performing thorough background investigations on employees who have access to cardholder data reduces the risk of unauthorized use of account numbers 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).</p>

Requirement	Guidance
<p><b>12.8</b> If cardholder data is shared with service providers, then contractually the following is required:</p> <p><b>12.8.1</b> Service providers must adhere to the PCI DSS requirements</p> <p><b>12.8.2</b> Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.</p>	<p>If a merchant or service provider shares cardholder data with a service provider, then the service provider receiving the cardholder data should sign a legal document that holds them responsible for complying with cardholder data security policies, and has them acknowledge this responsibility. This helps ensure that the continued protection of this data will be enforced by outside parties.</p>
<p><b>12.9</b> Implement an incident response plan. Be prepared to respond immediately to a system breach.</p> <p><b>12.9.1</b> (a) Create the incident response plan to be implemented in the event of system compromise.</p>	<p>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.</p>
<p>(b) Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)</p>	<p>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.</p>
<p><b>12.9.2</b> Test the plan at least annually</p>	<p>Without proper testing, key steps may be missed that could limit exposure during an incident.</p>
<p><b>12.9.3</b> Designate specific personnel to be available on a 24/7 basis to respond to alerts</p>	<p>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.</p>
<p><b>12.9.4</b> Provide appropriate training to staff with security breach response responsibilities</p>	
<p><b>12.9.5</b> Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.</p>	<p>These monitoring systems are designed to focus on potential risk to data and are critical in taking quick action to prevent a breach. <i>Ensure monitoring systems are included in incident response processes.</i></p>

Requirement	Guidance
<p><b>12.9.6</b> Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.</p>	<p>Incorporating “lessons learned” into the incident response plan after an incident helps keep the plan current and able to react to security trends</p>
<p><b>12.10</b> All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following:</p>	<p>A “connected entity” is any entity that is "upstream" and connected to a processor or service provider for purposes of receiving cardholder data, including processors, agents, sales organizations, and other service providers. This definition of "connected entities" does not include "downstream" entities such as merchants and other service providers and processors who originated the data and are now receiving it back from the entity in question. To manage these connected entities effectively, processors and service providers should have policies to guide them.</p>
<p><b>12.10.1.</b> Maintain a list of connected entities</p>	<p>An inventory list of connected entities should be maintained to provide information about each connection and to help troubleshoot, if needed.</p>
<p><b>12.10.2.</b> Ensure proper due diligence is conducted prior to connecting an entity</p>	<p>The policy should include a due diligence process, according to the due diligence deemed to be necessary by the company.</p>
<p><b>12.10.3.</b> Ensure the entity is PCI DSS compliant</p>	<p>The intent of this requirement is met if the company has a contract with the connected entity, per 12.8.1 above.</p>
<p><b>12.10.4.</b> Connect and disconnect entities by following an established process.</p>	<p>The policy should include a checklist of steps to occur in the connection and disconnection processes.</p>

## Guidance for Requirement A.1: PCI DSS Applicability for Hosting Providers

### **Requirement A.1: Hosting providers protect cardholder data environment**

As referenced in Requirement 12.8, all service providers with access to cardholder data (including hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that hosting providers must protect each entity's hosted environment and data. Therefore, hosting providers must give special consideration to the following:

Requirement	Guidance
<b>A.1</b> Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, as in A.1.1 through A.1.4:	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.
<b>A.1.1</b> Ensure that each entity only has access to own 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.
<b>A.1.2</b> Restrict each entity's access and privileges to own cardholder data environment only	To ensure that access and privileges are restricted such that each merchant or service provider only has access to their own cardholder data environment, consider the following 1) privileges of the merchant's or service provider's web server user ID, 2) permissions granted to read, write, and execute files, 3) permissions granted to write to system binaries, 4) permissions granted to merchant's and service provider's log files, and 5) controls to ensure one merchant or service provider cannot monopolize system resources.
<b>A.1.3</b> 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.
<b>A.1.4</b> 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 enable a process 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
<i>PCI Data Security Standard</i>	All merchants and service providers
<i>Navigating PCI DSS: Understanding the Intent of the Requirements</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Questionnaire Guidelines and Instructions</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Questionnaire A and Attestations</i>	All service providers; merchants <sup>9</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Merchants <sup>1</sup>
<i>PCI DSS Glossary, Abbreviations, and Acronyms</i>	All merchants and service providers

<sup>9</sup> 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.”