PCI Security Standards Council™

Standard:	PCI Data Security Standard (PCI DSS)
Version:	2.0
Date:	August, 2011
Author:	Wireless Special Interest Group (SIG) PCI Security Standards Council

Information Supplement: PCI DSS Wireless Guidelines

Document Changes

Date	Version	Description	Pages
August 2011	2.0	Updated to align with PCI DSS v2.0 requirements. Incorporated guidance for Bluetooth technologies.	

Table of Contents

1. Document Overview

1.1. Document purpose and Scope

This Information Supplement provides guidance and recommendations for deploying wireless networks including 802.11 Wi-Fi and 802.15 Bluetooth technologies, in accordance with the Payment Card Industry Data Security Standard (PCI DSS). The goal is to help organizations understand and interpret how PCI DSS applies to wireless environments, how to limit the PCI DSS scope as it pertains to wireless, and to provide practical methods and concepts for deployment of secure wireless in payment card transaction environments.

This document focuses on 802.11 Wi-Fi and 802.15 Bluetooth technologies, and does not cover cellular networks (GSM, GPRS, etc).

All references made to the PCI DSS in this document refer to PCI DSS version 2.0.

1.2. Audience

This guidance document is intended for organizations that store, process, or transmit cardholder data and that may or may not have deployed wireless technology, as well as assessors performing PCI DSS assessments pertaining to wireless.

2. Wireless Guidance Overview

PCI DSS wireless requirements can be broken down into the following two primary categories.

1. Generally applicable wireless requirements: All organizations should have these controls in place to protect their wired networks from attacks via rogue or unknown wireless access points (APs) and clients. These requirements are intended for all organizations wishing to comply with PCI DSS, *regardless of whether wireless technology is intentionally used in the CDE*.
2. Requirements applicable for “in scope” wireless networks and devices: All organizations that transmit payment card information over wireless technology should have these controls in place to protect those systems. The requirements are specific to the usage of wireless technologies that are in scope for PCI DSS compliance, namely those located within or connected to the cardholder data environment. These controls apply *in addition to* the generally applicable requirements outlined in 1 above.

2.1. Wireless Usage in the Cardholder Data Environment

The cardholder data environment (CDE) is comprised of people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data. PCI DSS applies to all system components included in or connected to the CDE. This section looks at some common wireless deployment scenarios and their associated scoping considerations.

In Figure 1 we see an example of a CDE consisting of a cabled network.

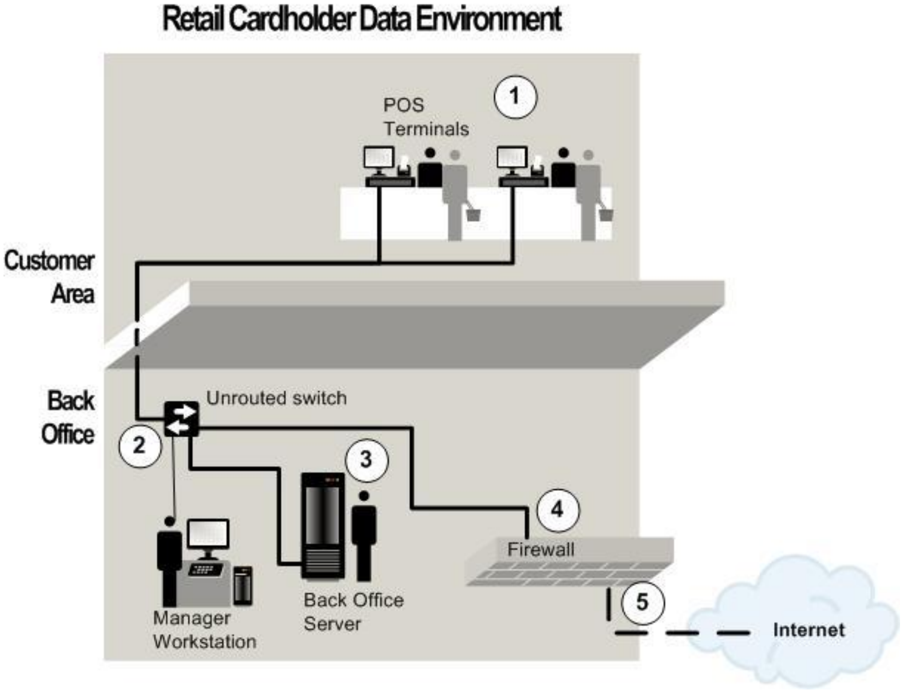

Figure 1: Example of cabled cardholder data environment

Figure 1 description:

1. *These are the point-of-sale terminals wherein the cardholder data enters the network.*
2. *This could be a hub, switch, or other device that acts to connect all devices to the same data environment. In this case, it transmits cardholder data.*
3. *This is a back-office server that is within the CDE by the fact that it is connected to the same cabled network, whether or not it stores cardholder data.*
4. *This is a firewall that demarcates the edge of the organization's CDE.*
5. *All traffic leaving the firewall to the Internet or elsewhere is encrypted and considered outside of this CDE.*

2.1.1. The "rogue" WLAN Access Point (AP) or Bluetooth Base

A rogue access point (AP) is any device that adds an unauthorized (and therefore unmanaged and unsecured) WLAN to the organization's network (see Figure 2 below). A rogue AP could be added by inserting a WLAN card into a back office server, attaching an unknown WLAN router to the network, adding a Bluetooth base, or by various other means.

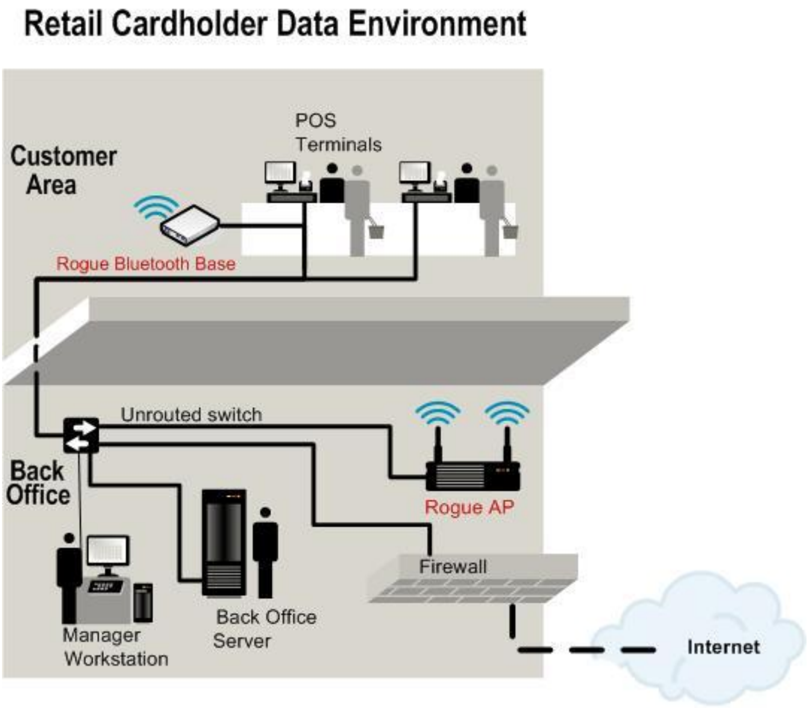

Figure 2: Rogue AP and Bluetooth base station added to the CDE

2.1.2. Adding a known WLAN to the CDE

In the case where an organization has decided to deploy a WLAN for any purpose whatsoever, and connects the WLAN to the CDE (see Figure 3), that WLAN is now in scope for PCI DSS.

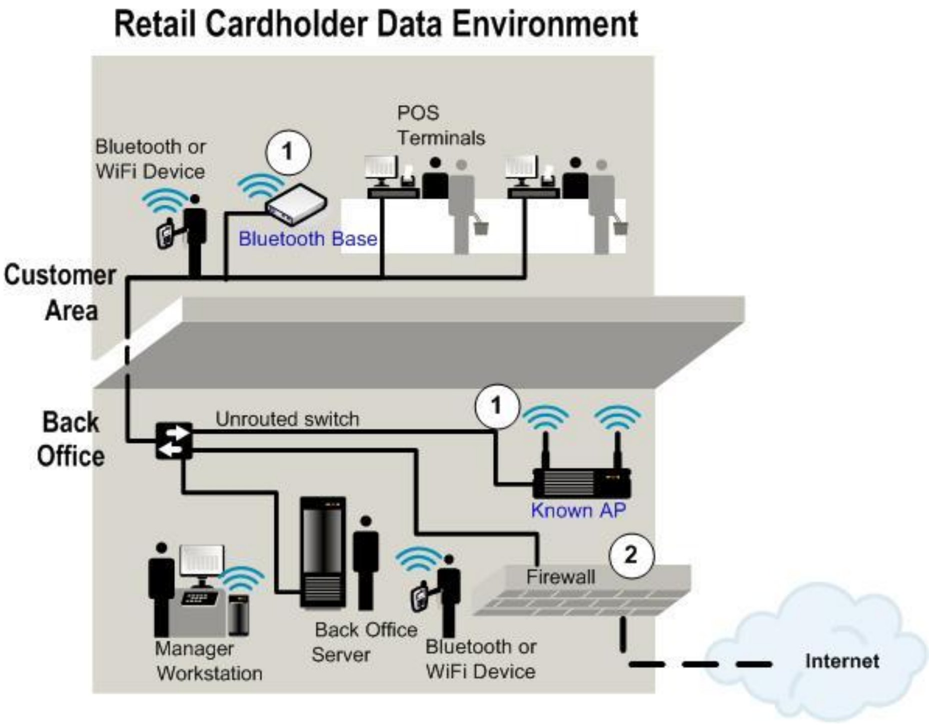

Figure3: CDE with an authorized WLAN and Bluetooth base station

Figure 3 description:

1. *In this case, the authorized WLAN access point (AP) and Bluetooth base are connected directly to the wired network within the CDE.*
2. *Even if an organization uses the wireless technology only for non-payment functions (for example, inventory control), and no cardholder data is being wirelessly transmitted, the wireless networks are connected to the CDE and are therefore in scope for PCI DSS.*

2.1.3. Adding a known WLAN outside *of the CDE*

In the case where a WLAN is added *outside* of the CDE (see Figure 4), and is appropriately segmented so that *no traffic whatsoever* passes between the WLAN and the CDE, that WLAN can be considered out of scope for PCI DSS. However, if the WLAN is connected to a firewall on the CDE, the firewall's configuration and the verification of proper network segmentation are in scope for both the PCI DSS and this document, even though the AP itself may be outside the scope of PCI DSS.

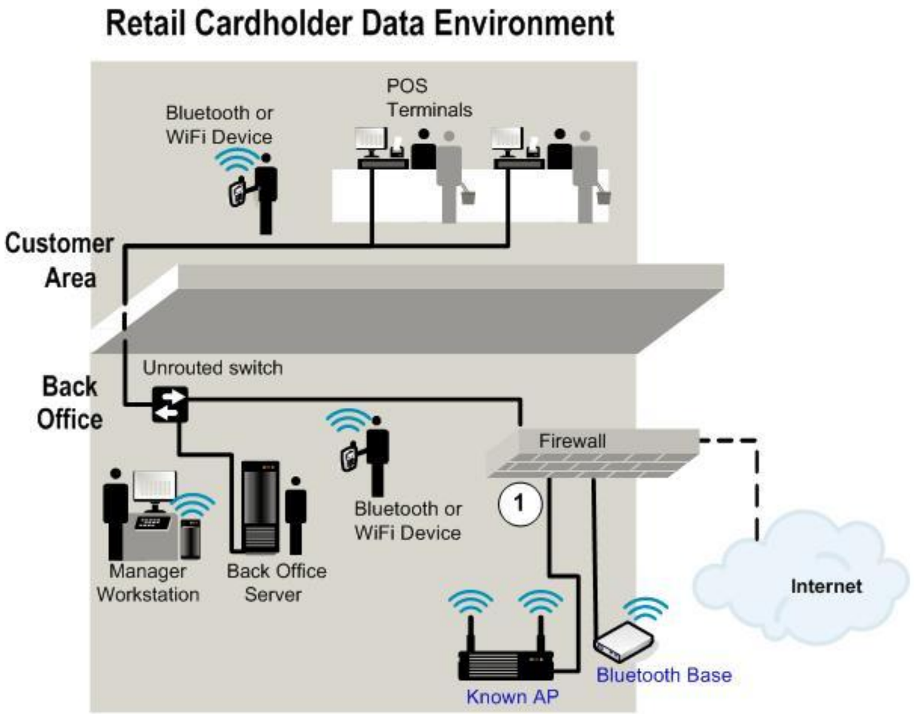

Figure 4: Wireless networks outside the CDE

Figure 4 description:

1. *In this case, the authorized wireless access point (AP) and Bluetooth base are segmented (isolated) from the CDE.*

2.2. How to use this guide

The following sections identify some of the key PCI DSS requirements related to wireless and provide recommendations for implementing wireless in a PCI DSS compliant manner. Note that the recommendations provided in this document are intended as guidance only and do not replace, supersede, or extend PCI DSS requirements.

Figure 5 shows a step-by-step decision process for complying with some of the core PCI DSS requirements related to wireless networks. The following sections provide specific guidance on the requirements identified in the flow chart, beginning with testing for the presence of rogue wireless technologies.

> ***Note:*** *PCI DSS requirements must be individually evaluated for each environment. The following guidance highlights only some of the PCI DSS requirements that may apply to a wireless implementation; each wireless implementation will need to be individually reviewed to determine how PCI DSS applies to that environment.*

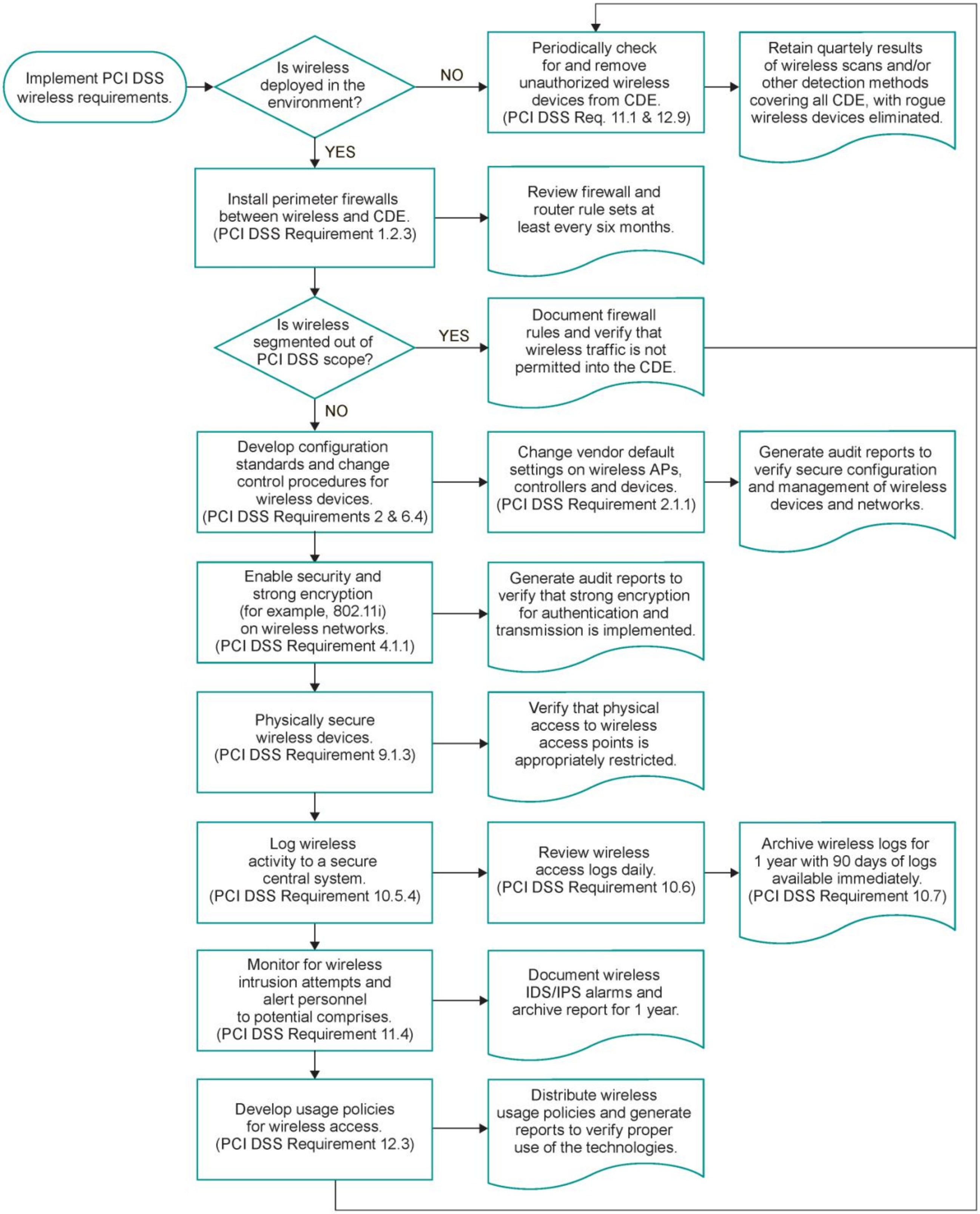
Implement PCI DSS wireless requirements.
Is wireless deployed in the environment?
NO
Periodically check for and remove unauthorized wireless devices from CDE. (PCI DSS Req. 11.1 & 12.9)
Retain quartely results of wireless scans and/or other detection methods covering all CDE, with rogue wireless devices eliminated.
YES
Install perimeter firewalls between wireless and CDE. (PCI DSS Requirement 1.2.3)
Review firewall and router rule sets at least every six months.
Is wireless segmented out of PCI DSS scope?
YES
Document firewall rules and verify that wireless traffic is not permitted into the CDE.
NO
Develop configuration standards and change control procedures for wireless devices. (PCI DSS Requirements 2 & 6.4)
Change vendor default settings on wireless APs, controllers and devices. (PCI DSS Requirement 2.1.1)
Generate audit reports to verify secure configuration and management of wireless devices and networks.
Enable security and strong encryption (for example, 802.11i) on wireless networks. (PCI DSS Requirement 4.1.1)
Generate audit reports to verify that strong encryption for authentication and transmission is implemented.
Physically secure wireless devices. (PCI DSS Requirement 9.1.3)
Verify that physical access to wireless access points is appropriately restricted.
Log wireless activity to a secure central system. (PCI DSS Requirement 10.5.4)
Review wireless access logs daily. (PCI DSS Requirement 10.6)
Archive wireless logs for 1 year with 90 days of logs available immediately. (PCI DSS Requirement 10.7)
Monitor for wireless intrusion attempts and alert personnel to potential comprises. (PCI DSS Requirement 11.4)
Document wireless IDS/IPS alarms and archive report for 1 year.
Develop usage policies for wireless access. (PCI DSS Requirement 12.3)
Distribute wireless usage policies and generate reports to verify proper use of the technologies.

Figure 5: PCI DSS wireless requirements

3. Generally Applicable Wireless Requirements

Wireless networking is a concern for all organizations that store, process, or transmit cardholder data and who therefore must adhere to PCI DSS. Even if an organization does not intentionally use any wireless technology, they must periodically verify that wireless technologies have not been introduced into their environment. Organizations that use wireless technology outside of their CDE must verify that all wireless networks (which include Wi-Fi and Bluetooth) are appropriately segmented from the CDE and that unauthorized wireless technology has not been introduced into the CDE.

While PCI DSS includes requirements for securing existing wireless technologies, it also recognizes there are risks beyond the intended use of wireless devices in an environment. PCI DSS therefore requires periodic detection and identification of unknown and potentially dangerous rogue wireless devices, as well as documented response procedures in the event unauthorized wireless devices are detected.

3.1. Maintain a hardware inventory

In order to answer the question "Are authorized wireless technologies deployed in my environment?" an organization must first identify the boundaries of their network(s) and have accurate, up-to-date network documentation. A complete, detailed hardware inventory is also strongly recommended. While PCI DSS requirements do not specifically call for such an inventory, it will be difficult for many organizations to verify whether a particular wireless device is a rogue or authorized device without having an inventory to reference it against. Maintaining detailed hardware inventories can also help the early detection of unauthorized devices, such as the addition of APs to the network or WLAN access cards inserted into existing systems.

Organizations with internet-facing systems within or connected to their CDE may also be required to undergo external vulnerability scans performed by an Approved Scanning Vendor (ASV). Per the *ASV Program Guide,* ASV scan solutions are required to scan any detected wireless access points visible from the Internet. Without an up-to-date device inventory, an organization would have to treat all detected wireless devices as rogue until they can verify whether each device is authorized.

Additionally, a device inventory is an important tool to facilitate an organization's efforts to validate the scope of their annual PCI DSS review. An up-to-date device inventory can be more easily verified and may help identify devices that were previously overlooked or that were mistakenly thought to be out of scope.

3.1.1. Recommendations

A. Maintain an up-to-date hardware inventory so that known APs and Bluetooth stations can easily be distinguished from rogue APs. Additionally, consider the use of additional physical or logical controls that prevent or alert personnel to the addition or removal of devices to networks or systems in the CDE.

B. Train and educate personnel on the risks of introducing unauthorized wireless devices to the network, and to immediately report if they notice the appearance of any "new" devices in their environment or if a device is missing or stolen.

3.2. Test for Unauthorized Access Points

The 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. If a wireless device or network is installed without the organization’s knowledge, it can allow an attacker to easily and “invisibly” enter the network.

The purpose of PCI DSS Requirement 11.1 (see Table 1) is to ensure that an unauthorized access point is not surreptitiously deployed in the environment. An attack utilizing an unauthorized access point could compromise the integrity of the network and the security of cardholder data.

PCI DSS Requirement	Testing Procedure
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*	**11.1.a** Verify that the entity has a documented process to detect and identify wireless access points on a quarterly basis.
	11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: • WLAN cards inserted into system components • Portable wireless devices connected to system components (for example, by USB, etc.) • Wireless devices attached to a network port or network device
	11.1.c Verify that the documented process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.
	11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.
	11.1.e Verify the organization’s incident response plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.

Table 1: PCI DSS Requirement 11.1

Requirement 11.1 identifies some of the methods that can be used, together or separately, to meet the intent of the requirement. Whichever methods are used, they must be appropriate for the particular environment and sufficient to detect and identify any unauthorized devices, including devices that are hidden within or attached to computers or other system components, as well as devices connected directly to a network port or network device, such as a switch or router. The presence of any such unauthorized device could provide an unauthorized access point into the environment.

It’s important to note that suitable detection methods for one environment may not be appropriate for another environment. Factors to consider when identifying appropriate methods for a particular environment include the size and complexity of the environment, the existence of any authorized wireless technologies, and any environment-specific characteristics that may influence the effectiveness of a particular method.

3.2.1. Automated Scanning Tools

PCI DSS Requirement 11.1 identifies wireless analyzers and wireless IDS/IPS as accepted scanning methods. Wired-side network scans may identify some but not all unauthorized wireless devices. For example, wired-side network scanning may identify the presence of a wireless access point connected into a wired network port, but would probably not detect a wireless access point attached via USB to an authorized system. However, detection and prevention technology is continually evolving, and the effectiveness of wired-side scans will need to be evaluated on an individual basis.

Wireless analyzers can range from freely available PC tools to commercial scanners and analyzers. The goal of all of these devices is to “sniff” the airwaves and “listen” for wireless devices in the area and identify them. Using this method, a technician or auditor can walk around each site and detect wireless devices. The person would then manually investigate each device to determine whether it allows access to the CDE and then classify each device as being either authorized, rogue, or a neighboring device that is outside of the organization’s environment. Often, wired-side and wireless-side scanning can be combined to provide an effective method for detecting unauthorized devices.

Wireless IDS/IPS may provide relief from manual scanning, yet the scale of the organization and volume of data may have additional considerations for some environments. Wireless IDS/IPS may provide additional benefit to organizations wishing to secure their existing wireless networks. Depending on how it is configured, a wireless IDS/IPS may be able to detect and/or block the presence of rogue devices immediately, helping to maintain the security of the wireless network. Wireless IDS/IPS can be configured to scan both internal and external wireless networks, and may be combined with a wired-side IDS/IPS to correlate traffic patterns across the two network types.

Network access control (NAC) solutions can differ greatly in functionality, and may provide a combination of device authentication to prevent unauthorized systems connecting to the network, as well as configuration management to prevent unauthorized devices being attached to authorized systems on the network.

3.2.2. Physical and Logical Inspection

While tools such as wireless IDS/IPS can be used to automate and centrally manage the scanning for rogue access points, physical intervention remains the ultimate response to remove the rogue device. Logical methods of blocking rogue devices (for example, MAC address filtering or IP address filtering) can provide immediate, remote intervention; but physically removing the unauthorized equipment is always the final goal.

In some environments, physical and/or logical inspections of system components and network infrastructure may also provide or contribute to an effective method to detect rogue devices. Physical and logical inspections of network access points and network devices, system components, and configurations may indicate whether unauthorized devices have been in any way attached, inserted or connected. However, it should be noted that while physical network and system inspections would provide a current view of connected devices, they would be unlikely to detect rogue devices that were previously connected and that had been removed prior to the inspection (and possibly re-connected after the inspection).

The specific characteristics of each environment will dictate the appropriate methods or combination or methods to provide sufficient assurance that rogue wireless access points have not been introduced. For example, in the case of a single, standalone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, performing a detailed physical inspection of the kiosk itself may provide sufficient assurance that a rogue wireless access point has not been attached or installed into that kiosk. However, in an environment with multiple network nodes, it becomes more difficult to perform a detailed physical inspection due to the number of system components and network points where a rogue wireless device could be installed or hidden. In this case, it may be beneficial to combine one or more methods, such as performing physical system inspections in conjunction with the results of a wireless analyzer.

Because rogue devices can potentially show up in any location at any time, the detection process must be sufficient to encompass all system components and facilities at least quarterly. If during the annual PCI DSS annual compliance assessment, the assessor chooses to review a sample of locations as part of their validation of the organization's process, the sample must be sufficient to provide assurance that the process is implemented as expected across all locations.

3.2.3. Review and Follow-up Action

Although PCI DSS does not specify how an organization should record the results of their wireless detection process, it is a critical part of the process that the results are reviewed and appropriate action taken to mitigate the risk of unauthorized devices. An organization's incident response plan (per PCI DSS Requirement 12.9) should contain documented procedures to be followed in the event an unauthorized wireless access point is detected.

Where automated monitoring or scanning tools are used (for example, wireless IDS/IPS, NAC, etc.), they should be configured to generate alerts to notify personnel and initiate the response process. Procedures for reporting and responding to unauthorized devices detected during physical or logical inspections, or via manual scanning methods, should also be defined and implemented.

The response to unauthorized wireless devices should include action to remove the device and any corrective controls as appropriate to prevent a recurrence. In some instances, additional testing or rescans of the environment may be warranted to ensure the threat has been mitigated.

3.2.4. Recommendations

A. Identify methods and processes that are adequate and appropriate for the particular environment—for example, a centrally managed wireless IDS/IPS may be useful in a large, distributed environment, while a combination of manual wireless scans and physical inspections may be appropriate for a smaller, isolated location.

B. Implement controls to restrict physical and logical access to network entry points.

C. Combine manual physical and/or logical inspections of systems and network infrastructure with automated network monitoring and/or scanning, as appropriate.

D. If using automated tools (such as wireless IDS/IPS, NAC, etc.), enable automatic containment mechanisms to immediately block access to unauthorized wireless connections.

E. Ensure that incident-response procedures include the reporting and immediate physical removal of all rogue devices

F. Train and educate personnel on the risks of introducing unauthorized wireless devices to the network, and to immediately report if they notice the appearance of any 'new' devices in their environment.

3.3. Segment wireless networks

PCI DSS Requirement 1.2.3 (Table 2) mandates that firewalls be installed between any wireless networks and the CDE. The intent of this requirement is to prevent unauthorized individuals with access to the wireless network from connecting to the CDE and potentially compromising cardholder data.

PCI DSS Requirement	Testing Procedure
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	**1.2.3** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Table 2: PCI DSS Requirement 1.2.3

Because wireless networks are considered “public” networks, perimeter firewalls need to be implemented between all wireless networks and the CDE, regardless of the purpose of the wireless network. Wireless networks that are not in scope for PCI DSS must be completely isolated from the CDE, such that no traffic is permitted between the CDE and the wireless network. An example of how an untrusted wireless network may be isolated from the CDE is shown in Figure 6 below.

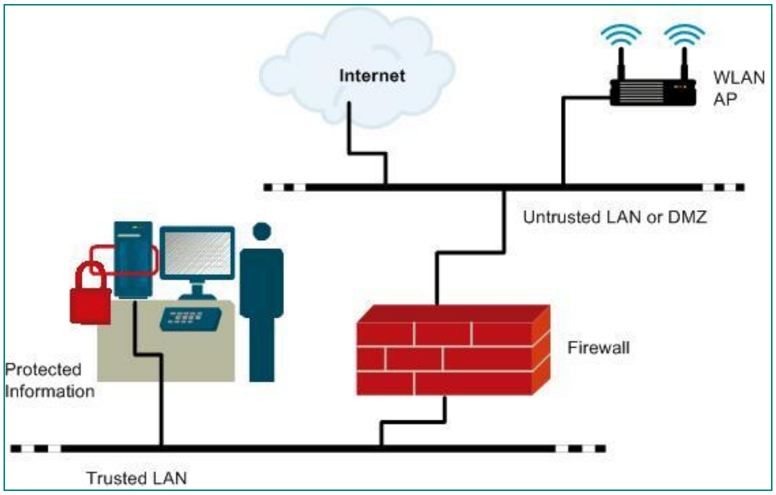

Figure 6: Illustration of AP outside of the CDE

If a wireless network is used for cardholder data, or is otherwise connected to or considered to be part of the CDE, firewalls are still needed between the wireless access points and systems in the CDE. If there is a business need for traffic to pass between the wireless network and the cardholder data environment, such traffic must be defined and controlled in accordance with PCI DSS Requirement 1.

At a high level, the firewalls between the CDE and wireless networks should perform the following general functions:

- Completely isolate out-of-scope wireless networks and prevent any traffic from entering the CDE by filtering wireless packets.
- Perform stateful inspection of connections between in-scope wireless networks and systems in the CDE, and restrict all traffic to that which is necessary for the CDE.
- Log traffic allowed and denied by the firewall.

PCI DSS Requirement 1.1.6 requires that all firewall and router rule sets be reviewed and verified at least every six months. If a firewall is being used to segment a wireless network from other systems, protocols and/or applications in the CDE, the default policy for the firewall should be to block all packets and connections into the CDE unless the traffic type and connection has been specifically permitted. Wireless traffic should explicitly be denied by default. Outbound traffic filtering can be used to further secure the networks and reduce the likelihood of internally based attacks.

As a general rule, any protocol or traffic that is not used or is not needed in the CDE should be blocked. This will result in reduced risk of attack as well as reduced traffic in the CDE, thus making it easier to control and monitor.

3.3.1. Recommendations

A. Combine a stateful packet inspection firewall with a wireless IDS/IPS to block wireless traffic from entering the CDE.

B. Ensure the effectiveness of any segmentation controls used to isolate wireless networks from the CDE. Don’t rely solely on VLAN-based segmentation or MAC address filters for segmenting wireless networks— a firewall implementation is still required per PCI DSS Requirement 1.2.3.

C. Minimize the amount of traffic that is permitted into or out of the CDE to only that which is absolutely necessary.

D. Log all traffic flows between wireless networks and the CDE.

4. Applicable Requirements for In-scope Wireless Networks

As discussed in Section 3, certain PCI DSS requirements related to wireless technology apply even if there are no wireless networks in scope—including the use of firewalls between wireless networks and the CDE (Requirement 1.2.3) and testing for the presence of rogue wireless devices (Requirement 11.1).

PCI DSS compliance for environments that use wireless networks as a part of the CDE requires additional controls to address wireless-specific technologies and processes such as:

1. Physical security of wireless devices;
2. Changing default passwords and settings and securely configuring wireless devices;
3. Logging of wireless access and intrusion prevention;
4. Strong authentication and encryption;
5. Use of strong cryptography and security protocols; and
6. Development and enforcement of wireless usage policies.

This section will cover each of these requirements in order.

Note that risks in wireless networks essentially include the risks associated with operating a wired network, *plus* the additional risks introduced by weaknesses in wireless protocols. Threats and vulnerabilities of wireless systems are discussed in multiple reference documents listed at the end of this document.

The following guidance highlights only some of the PCI DSS requirements that may apply to a wireless implementation; each wireless implementation will need to be individually reviewed to determine how PCI DSS applies to that environment.

4.1. Physical security of wireless devices

PCI DSS promotes the need for physical security surrounding wireless access points, gateways, and handheld devices (Table 3). The focus of this requirement is to prevent unauthorized persons from using unattended wireless devices to gain access to network resources, or connecting their own devices to the wireless network in order to gain unauthorized access. The security of devices that are publically accessible or provide access to critical components should be of particular concern. For example, the use of a physical cage may not be necessary for APs that are located in a secure data center, but may be justified for APs in public or semi-public areas, or that are otherwise deemed to be a high risk.

An obvious risk associated with insufficient physical security (other than theft) is the ability for an unauthorized person to reset an AP to its factory default settings. The reset function poses a particular problem because, by returning the AP to its default factory settings, it allows an individual to negate any security settings that administrators have configured in the AP. The default settings generally do not require an administrative password, for example, and may disable encryption. An individual can reset the configuration to the default settings simply by inserting a pointed object such as a pen into the reset hole and pressing. If a malicious user gains physical access to the device, that individual can exploit the reset feature and cancel any security settings on the device. Additionally, an AP reset can be invoked over the management interface or by using a serial console interface on the AP. An attacker with physical access could connect to a physical port on the device and bypass network access controls, which is why PCI

DSS requires that adequate mechanisms be in place to prevent unauthorized physical access to wireless devices.

PCI DSS Requirement	Testing Procedure
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/ communications hardware, and telecommunication lines.	**9.1.3** Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.

Table 3: PCI DSS Requirement 9.1.3

Although PCI DSS does not mandate how wireless devices are to be secured, there are many ways to implement physical security.

Options for securing wireless devices may include physically restricting access (e.g., by mounting APs or base stations high up on the ceiling) and disabling the console interface and factory reset options through use of a tamper-proof chassis. Many enterprise APs are equipped with special mounting brackets that prevent access to the network cable.

Securing handheld wireless devices and laptops may be more difficult since physical access to these devices is typically needed to perform job functions. Such devices should be physically secured when not in use or if left unattended in a public area.

Common-sense precautions such as ensuring that pre-shared keys (PSKs) and passwords are not located near the device or insecurely stored on the device are a must. Maintaining an inventory of wireless devices and being able to track and report missing devices is also recommended.

4.1.1. Recommendations

A. Mount APs on (or in) ceilings and walls that do not allow easy physical access, or locate in secure areas, such as locked closets or server rooms.

B. Use APs with tamper-proof chassis and mounting options that prevent physical access to ports and reset features.

C. Review signal settings and physical placement of APs to provide maximum coverage for the desired service area while minimizing broadcast range outside of the environment.

D. Secure handheld devices with strong passwords and always encrypt PSKs if cached locally.

E. Enable automatic lockouts on handheld devices after a defined idle period, and configure devices to require a password when powering on.

F. Use a wireless monitoring system that can track and locate all wireless devices and report if one or more devices are missing.

4.2. Change default settings and securely configure wireless devices

If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, capture data and passwords, and easily enter and attack the network. Changing default settings (Table 4), including passwords, encryption settings, reset functions, automatic network connection functions, factory-default shared keys, and Simple Network Management Protocol (SNMP) strings, will help eliminate many of the vulnerabilities that can impact the security of the CDE through unauthorized wireless access.

PCI DSS Requirement	Testing Procedure
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**2.1.1** Verify the following regarding vendor default settings for wireless environments:
	2.1.1.a Verify encryption keys were changed from default at installation, and are changed anytime anyone with knowledge of the keys leaves the company or changes position
	2.1.1.b Verify default SNMP community strings on wireless devices were changed.
	2.1.1.c Verify default passwords/passphrases on access points were changed.
	2.1.1.d Verify firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.
	2.1.1.e Verify other security-related wireless vendor defaults were changed, if applicable.

Table 4: PCI DSS Requirement 2.1.1

Each wireless device comes with its own default settings, some of which inherently contain security vulnerabilities. The administrator password is a prime example. On some APs, the factory default configuration does not require a password (or the password field is blank). Other APs might have simple and well-documented passwords (for example, “password” or “admin”). Unauthorized users can easily gain access to the device’s management console if default settings are left unchanged. Similarly, many wireless APs have a factory default setting that allows unencrypted wireless access. Some APs might be pre-configured for WEP access with simple keys like “111111”.

4.2.1. Network protocols and identifiers

Some wireless APs use SNMP agents, which allow network management software tools to monitor the status of wireless APs and clients. The first two versions of SNMP, SNMPv1 and SMPv2, support only trivial authentication based on plain-text community strings and, as a result, are fundamentally insecure. SNMPv3, which includes mechanisms to provide strong security, is highly recommended. If SNMP is not required on the network, the organization should simply disable SNMP altogether. It is common knowledge that the default SNMP community string that SNMP agents commonly use is the word “public” with assigned “read” or “read and write” privileges. Leaving this well-known default string unchanged leaves devices vulnerable to attack. If an unauthorized user were to gain access and had read/write privileges, that user could write data to the AP, resulting in a data-integrity breach. Organizations that require SNMP should change the default community string as often as needed to a strong community string. Privileges should be set to “read only” wherever possible.

All Wi-Fi APs have a default service set identifier (SSID). The SSID is an identifier that is sometimes referred to as the “network name” and is often a simple ASCII character string. The SSID is used to assign an identifier to the wireless network (service set). Clients wishing to join a network can scan the area for available networks and join by providing the correct SSID. Disabling the broadcast SSID feature in the APs causes the AP to ignore the message from the client and forces it to perform active scanning (probing with a specific SSID). The default values of SSID used by many 802.11 wireless LAN vendors have been published and are well known to would-be adversaries. The default values should be changed (always a good security practice) to prevent easy access. Suppressing the SSID is not necessarily a security mechanism as a hacker can sniff the SSID using fairly trivial techniques. However, broadcasting an SSID that advertises the organization’s name or is easily identifiable with the organization is not recommended.

Setting the transmit power to the lowest power needed to accomplish to job prevents the signal from leaving the facility.

4.2.2. Secure configuration settings

When configuring the wireless AP, ensure that the device’s monitoring and logging capabilities are synchronized for proper traceability. This is done through synchronizing the AP’s clock with the clocks of the other firewalls, routers, and servers. Without the clocks being synchronized, it is not possible to discern which logging events on the AP match logged events in other devices.

Disable all unnecessary hardware, services, and applications that the AP might have shipped with. Check for the following protocols to ensure that they aren’t configured unless absolutely necessary:

- Dynamic Host Configuration Protocol (DHCP) (for assigning IP addresses on the fly);
- HTTP SSL (for protected web pages); and
- Wireless zero configuration service (for those APs and devices connecting to them) that run on Windows OS.

4.2.3. Recommendations

A. Ensure that all default PSKs are changed. Enterprise mode is recommended.

B. Disable SNMP access to remote APs if possible. If not, change default SNMP passwords and use SNMPv3 with authentication and privacy enabled.

C. Change the SSID. Do not advertise organization names in the SSID broadcast, or include information that may be useful for attackers (such as the location of the AP).

D. Synchronize all AP clocks with other network devices in the organization.

E. Disable all unnecessary applications, ports, and protocols.

For Bluetooth devices[1]:

F. Choose PIN codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes.

G. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing.

H. Ensure that link keys are based on combination keys rather than unit keys. Do not use unit keys.

I. For v2.1 devices using Secure Simple Pairing, do not use the "Just Works" model.

J. Perform service and profile lockdown of device Bluetooth stacks. Do not allow the use of multiple profiles in the unit.

K. In the event a Bluetooth device is lost or stolen, immediately unpair the missing device from all other Bluetooth devices with which it was previously paired.

4.3. Wireless intrusion prevention and access logging

Intrusion detection (Table 5) is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents which are violations or imminent threats of violation of security policies, acceptable use policies, or standard security practices. An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is a system that has all the capabilities of an IDS and can also attempt to stop possible incidents. These systems are well established in Wi-Fi (802.11) configurations but are limited in supporting Bluetooth (802.15) environments because of the volume of such devices and the nature of the technology.

PCI DSS Requirement	Testing Procedure
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	**11.4.a** Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment is monitored.
	11.4.b Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

Table 5: PCI DSS Requirement 11.4

[1] NIST Special Publication 800-121 Guide to Bluetooth Security, September 2008

Wireless IDS/IPS provides several types of security capabilities intended to detect misconfiguration, misuse, and malicious activity. These capabilities can be grouped into three categories:

(i) Rogue wireless containment;

(ii) Detection of unsafe activity or configurations; and

(iii) Detection of denial of service attacks and wireless intrusion attempts.

4.3.1. Rogue wireless containment

Unauthorized wireless devices connected to the CDE must be detected and disabled. A wireless IPS should be able to find these rogue devices even when they are configured to not broadcast information about themselves or are present in isolated network segments. In addition to rogue containment, organizations should evaluate the automatic device classification capabilities of the wireless IDS/IPS for situations when connectivity cannot be determined. A wireless IDS/IPS should be able to observe all APs and clients, on all operational channels, and classify each device as authorized, unauthorized/rogue or neighboring. Many wireless IPS systems provide the ability to prevent clients from associating with an unauthorized AP or can disable an ad-hoc network. However, efficacy of these techniques varies widely, and while they can provide adequate temporary mitigation of the risk, unauthorized devices should be physically removed from the CDE as soon as possible.

4.3.2. Detection of unsafe activity or configurations

A wireless IDS/IPS can detect misconfigurations and unsafe activity by monitoring and analyzing wireless communications. Most can identify APs and clients that are not using the proper security controls. This includes detecting misconfigurations and the use of weak WLAN protocols, and is accomplished by identifying deviations from organization-specific policies for settings such as encryption, authentication, data rates, SSID names, and channels. For example, they could detect that a wireless device is using WEP instead of WPA2. Some wireless IDS/IPS use anomaly-based detection methods to detect unusual WLAN usage patterns. For example, a higher than usual amount of network traffic between a wireless client and an AP might be an indication that one of the devices is compromised, or that unauthorized parties are using the WLAN. Some systems can also alert if any WLAN activity is detected during off-hours periods.

4.3.3. Detection of denial of service attacks and wireless intrusion attempts

A wireless IDS/IPS can also analyze wireless traffic to look for malicious activity such as denial of service (DoS) and individual attacks on devices. As with a wired IDS/IPS, the system looks for attempts to disrupt the wireless network or a device on the network, or to gain unauthorized access to the network. If these detections are signature-based, organizations should update the signatures whenever new threats are discovered.

4.3.4. Threat identification and logging

Most wireless IDS/IPSs can identify the physical location of a detected threat by using signal strength triangulation. This is performed by estimating the threat's approximate distance from multiple sensors by the strength of the threat's signal received by each sensor, and then calculating the physical location at which the threat would be the estimated distance from each sensor. This allows an organization to remediate more easily by pinpointing the location of a rogue device—for those systems that do "radio location."

In order for the organization to be able to *use* the information collected from wireless IDS/IPS, the information has to be properly logged and correlated. This means that the logs from the IDS/IPS need to be coordinated with other logging systems on the network (if there are any). In this case, the organization should ensure that at least the following log settings are coordinated correctly:

- The log file prefix (used to identify the device conducting the logging)
- The level of logging (the types of events and amount of detail to log)
- The log auto-roll setting (whether a new log file is created when the device is restarted, or the maximum log size is reached)
- The log maximum (log age in days)

Once the information provided by the IDS/IPS is collected and organized, remember to **read the IDS/IPS reports.** If there are anomalies, they must be resolved. It is *not* enough to merely purchase and properly configure an IDS/IPS; the organization's policies and procedures must include reviewing and acting on the logs provided by this and other key monitoring devices. [See PCI DSS Requirement 10 for details of log configuration and management controls.]

4.3.5. Recommendations

A. Use a centrally controlled wireless IDS/IPS to monitor for unauthorized access and to detect rogue and misconfigured wireless devices.

B. Enable historical logging of wireless access that can provide granular wireless device information and store event logs and statistics for at least 12 months (with 90 days immediately accessible).

C. Enable IPS features to automatically disable rogue wireless devices connecting to the CDE as well as accidental or malicious associations of wireless clients.

D. Ensure the IPS signature set is regularly updated as new threats are discovered.

E. Coordinate and correlate wireless logging events with other networking devices within the environment.

F. Implement processes and policies that include regularly reviewing and acting on the data provided by the IDS/IPS.

4.4. Strong wireless authentication and encryption

By 2001, a series of independent studies from various academic and commercial institutions had identified weaknesses in Wired Equivalent Privacy (WEP), the original native security mechanism for WLANs, in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wi-Fi specification. These studies showed that, even with WEP enabled, an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to the wireless network.

In 2003, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA) as a strong, standards-based interoperable Wi-Fi security specification. WPA provides assurance that data will remain protected and that only authorized users may access the network. WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption that changes keys used for encryption on a per-packet basis.

In 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), the second generation of WPA security. Like WPA, WPA2 provides Wi-Fi users with a high level of assurance that their data will remain protected and that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard ratified in June 2004. WPA2 uses the Advanced

Encryption Standard (AES) for data encryption and is eligible for FIPS (Federal Information Processing Standards) 140-2 compliance.

PCI DSS version 2.0 specifies that WEP must not be used as a security control for wireless networks. PCI DSS compliance requires the use of robust encryption and authentication as provided by the IEEE 802.11i Standard (Table 6). The Wi-Fi Alliance certifies products as WPA or WPA2 compatible for interoperability based on the 802.11i Standard.

PCI DSS Requirement	Testing Procedure
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. ***Note:*** *The use of WEP as a security control was prohibited as of 30 June 2010.*	**4.1.1** For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.

Table 6: PCI DSS Requirement 4.1.1

4.4.1. WPA and WPA2 modes and encryption

There are two modes in WPA and WPA2 – Enterprise and Personal (Table 7). Both provide an authentication and encryption solution.

Mode	WPA	WPA2
Enterprise	Authentication: IEEE 802.1X/EAP Encryption: TKIP/MIC	Authentication: IEEE 802.1X/EAP Encryption: AES-CCMP
Personal	Authentication: PSK Encryption: TKIP/MIC	Authentication: PSK Encryption: AES-CCMP

Table 7: The two modes in WPA

Personal mode is designed for home and small office/home office (SOHO) users who do not have authentication servers available. It operates in an unmanaged mode that uses a pre-shared key (PSK) for authentication instead of IEEE 802.1X. This mode uses applied authentication in which a pass-phrase (the PSK) is manually entered on the access point to generate the encryption key. Consequently, it does not scale well in the enterprise. The PSK is typically shared among users. Weak passphrases are vulnerable to password cracking attacks. To protect against a brute-force attack, a truly random passphrase of 13 or more characters (selected from the set of 95 permitted characters) is recommended.

Enterprise mode operates in a managed mode to meet the rigorous requirements of enterprise security. It leverages the IEEE 802.1X authentication framework, which uses an Extensible Authentication Protocol (EAP) type, with an authentication server to provide strong mutual authentication between the client and authentication server. In this mode, each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP encryption is used. TKIP employs an encryption cipher that issues encryption keys for each data packet communicated in each session of each user, making the encryption code extremely difficult to break. For WPA2, AES encryption is used. AES is stronger than TKIP, thus providing additional network protection.

Recent attacks against the TKIP encryption algorithm have revealed some flaws in the protocol that can allow an attacker to decrypt small frames encrypted using TKIP, such as Address Resolution Protocol (ARP) frames, in about 15 minutes. Further, the attacks revealed that it is possible to reuse the compromised encryption keystream to inject 7-15 arbitrary packets into the network using Quality of Service (QoS) mechanisms without triggering the replay-protection countermeasures available in TKIP. While the attack does not lead to a compromise of the PSK, it is recommended that organizations use AES encryption, which is immune to this attack.

The Wi-Fi Alliance has announced the inclusion of additional EAP types for its WPA and WPA2 Enterprise certification programs. This was to ensure that WPA Enterprise-certified products can interoperate with one another. Previously, only EAP-TLS (Transport Layer Security) was certified by the Wi-Fi Alliance. Table 8 below illustrates the popular EAP types certified by the Wi-Fi Alliance, along with a comparison of features.

WPA Enterprise Mode	PEAP	EAP-TLS	EAP-TTLS
User Authentication Database and Server	OTP, LDAP, NDS, NT Domains, Active Directory	LDAP, NT Domains, Active Directory	OTP, LDAP, NDS, NT Domains, Active Director
Native Operating System Support	Windows XP, 2000	Windows XP, 2000	Windows XP, 2000, ME, 98, WinCE, Pocket PC2000, Mobile 2003
User Authentication Method	Password or OTP	Digital Certificate	Password or OTP4
Authentication Transaction Overhead	Moderate	Substantial	Moderate
Management Deployment Complexity	Moderate Digital Certificate For Server	Substantial Digital Certificate Per Client and For Server	Moderate Digital Certificate For Server
Single Sign On	Yes	Yes	Yes

Table 8: WPA Enterprise mode security

ANS X9.112 defines similar data confidentiality, entity authentication and data integrity requirements with an additional requirement for *security encapsulation*. Security encapsulation is the independent protection of specific data elements within another security protocol, such as separate PIN encryption at the point of entry within the WPA protocol.

4.4.2. Bluetooth pairing

In Bluetooth, pairing is controlled in an ad-hoc fashion, allowing different devices to establish connections. Pairing should be controlled and mutual authentication should be practiced. It is never a good idea to respond to any request for pairing or PIN unless the user has initiated the pairing sequence.

4.4.3. Recommendations

A. WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption is recommended for WLAN networks.

B. It is recommended that WPA2 Personal mode be used with a minimum 13-character random passphrase and AES encryption.

C. Pre-shared keys should be secured and changed on a regular basis.

D. Centralized management systems that can control and configure distributed wireless networks are recommended.

E. The use of WEP as a security control is prohibited after June 30, 2010.

For Bluetooth[2]:

F. Ensure device mutual authentication is performed for all accesses

G. Enable encryption for all broadcast transmissions (Encryption Mode 3).

H. Configure encryption key sizes to the maximum allowable.

I. Establish a “minimum key size” for any key negotiation process. Keys should be at least 128 bits long

J. For Bluetooth: Use application-level (on top of the Bluetooth stack) authentication and encryption for sensitive data communication such as SSL.

K. Perform pairing as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry and intercept Bluetooth pairing messages.

***Note:** A “secure area” is defined as a non-public area that is indoors away from windows in locations with physical access controls.*

L. Users should not respond to any messages requesting a PIN, unless the user has initiated a pairing and is certain the PIN request is being sent by one of the user’s devices.

M. Use only Security Mode 3 and 4. Modes 1 and 2 should not be allowed. Security Mode 3 is preferred but v.2.1 devices cannot use Security Mode 3.

N. Users should not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, or images.

O. All Bluetooth profiles except for Serial Port Profile should be disabled at all times, and the user should not be able to enable them

[2] NIST Special Publication 800-121 Guide to Bluetooth Security, September 2008

4.5. Use of strong cryptography for transmission of cardholder data

In addition to encrypting and authenticating wireless LANs using WPA2 or secure pairing, wireless networks are considered to be public networks This means all cardholder data must be encrypted as required in PCI DSS Requirement 4.1 if it is to be transmitted over a wireless network (Table 9). Encryption methods can include, but are not limited to, SSL/TLS, IPSEC, and WPA2-AES.

PCI DSS Requirement	Testing Procedure
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:* - The Internet - Wireless technologies, - Global System for Mobile communications (GSM) - General Packet Radio Service (GPRS).	**4.1** Verify the use of security protocols wherever cardholder data is transmitted or received over open, public networks. Verify that strong cryptography is used during data transmission, as follows:
	4.1.a Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit.
	4.1.b Verify that only trusted keys and/or certificates are accepted.
	4.1.c Verify that the protocol is implemented to use only secure configurations, and does not support insecure versions or configurations.
	4.1.d Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.)
	4.1.e For SSL/TLS implementations: ▪ Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). ▪ Verify that no cardholder data is required when HTTPS does not appear in the URL.

Table 9: PCI DSS Requirement 4.1

Figure 7 shows a wireless "hotspot" example using an SSLv3 HTTPS portal. In this example, wireless technology is used to conduct on-line payment card purchases over a "wireless hotspot network." Public locations such as airports, cafés, etc. will often provide an open wireless service which, when connected to, presents users with an HTTPS/SSL web page that allows them to purchase access to the internet. This process is analogous to purchasing merchandise on the Internet.

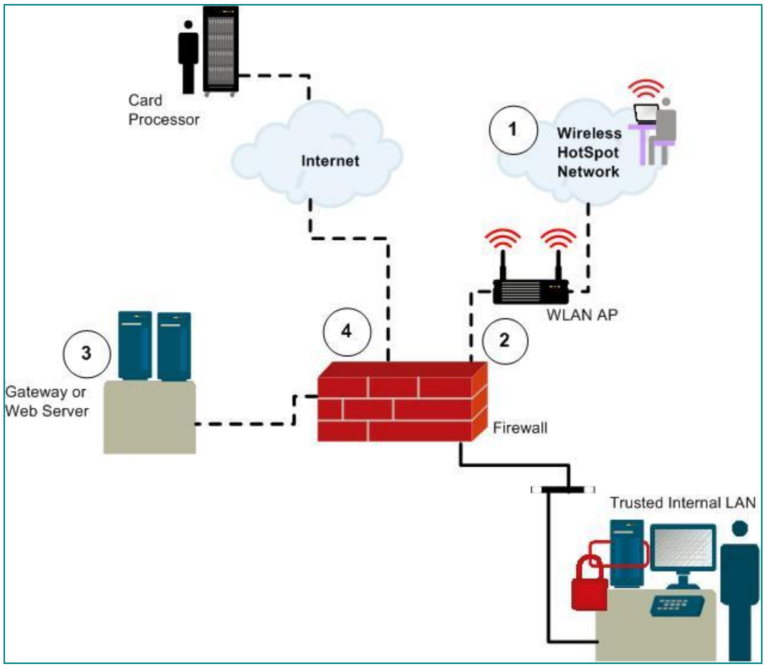

Figure 7: Wireless "Hotspot" example with SSLv3 HTTPS portal

Figure 7 description:

1. *The hotspot guest connects through the access point over a Wi-Fi network connected to the firewall's external LAN port using SSLv3 and TLS.*
2. *The firewall's LAN port is configured for NAT as well as "Deny All," with only those exceptions that must be in place for the transaction to occur.*
3. *The gateway or web server that processes the transaction uses SSL or a VPN connection.*
4. *The Internet port of the firewall is also configured for NAT as well as "Deny All,", with only those exceptions that must be in place for the transaction to occur.*

The dashed line signifies that the traffic contains payment card information and is encrypted.

An example of a multi-service wireless network with both public and POS services is shown in Figure 8. The guest traffic could be open or SSL as in Figure 7, the "Hotspot" example. The secure application traffic could be encrypted using IPSec or end-to-end WPA2-AES. In this example, the guest wireless network is treated as an "untrusted" network and is segmented from the corporate wireless network using a firewall.

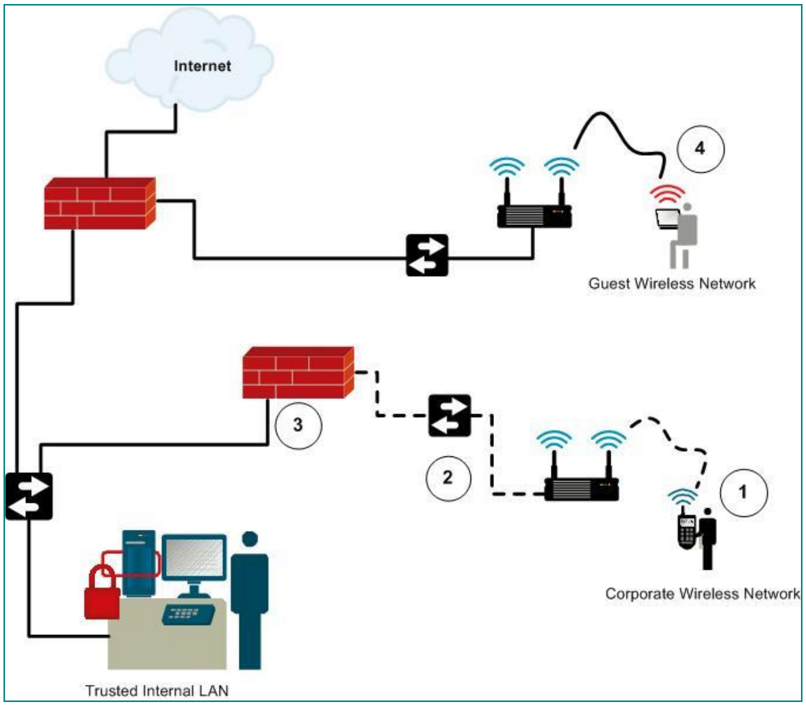

Figure 8: Secure Application Traffic separated from guest wireless traffic

Figure 8 description:

1. *Secure corporate wireless devices connect to the private WLAN through an AP. The dashed line signifies that the information flowing out through this segment is encrypted.*
2. *Secure application traffic tunnels are created through the IDF switches to an internal firewall. The dashed line signifies that the information flowing out through this segment is encrypted.*
3. *The firewall is the termination point for encrypted traffic. The firewall's connection rules also ensure that traffic flowing between the secure application and the secure wireless device traverse no other path than this one.*
4. *Guest traffic attaches through segmented wireless APs.*

SSLv3 is recommended as it supports a range of cipher suites that define the key-establishment algorithm, the encryption cipher, the hash function, and their parameters. Historically, SSLv2 supported older encryption ciphers (e.g., RC2 and DES) and cryptographic key lengths (e.g., 512-bit RSA and 512-bit DH) that are inappropriate for today's networks.

IPSec supports several security associations that define the cryptographic algorithms for the IP authentication header (AH) and the IP encapsulating security payload (ESP). Historically IPSec supports older algorithms (e.g., DES) with cryptographic strengths (e.g., 56-bit DES) that are inappropriate for today's networks.

Table 10 provides information on relative cryptographic strengths, based on NIST SP 800-57.

Cryptographic Strength	Symmetric Algorithm	Hash Algorithm	ECC Algorithms	RSA/DSA/DH Algorithms
56-bits	DES	-	-	-
80-bits	3DES-2K	SHA-1 (160)	160-bits	1024-bits
112-bits	3DES-3K	SHA-2 (224)	224-bits	2048-bits
128-bits	AES-128	SHA-2 (256)	256-bits	3072-bits
192-bits	AES-192	SHA-2 (384)	384-bits	7680-bits
256-bits	AES-256	SHA-2 (512)	512-bits	15360-bits

Table 10: Relative Cryptographic Strengths

4.5.1. Recommendations

A. Use only strong security protocols, such as SSLv3.

B. When possible, use at least 256-bit encryption.

C. Physically segment unsecured wireless networks from secured networks

4.6. Development and enforcement of wireless usage policies

The PCI DSS mandates the need for acceptable usage policies and procedures (Table 11), which include those for wireless devices. The importance here is that organizations understand and define how wireless is to be used within their environment, how it is to be secured and deployed, and how the organization will address incidents as they occur. Another important aspect to be addressed in the policy is how employees can and should use their authorized wireless devices. For example, if employees receive laptops, they need to understand the acceptable usage and responsibilities associated with wireless networking. Employees also need to understand how to properly protect, access, and store wireless devices.

PCI DSS Requirement	Testing Procedure
12.3 Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following (Requirements 12.3.1 – 12.3.10).	**12.3** Obtain and examine the usage policies for critical technologies and perform the following (Requirements 12.3.1 – 12.3.10).

Table 11: PCI DSS Requirement 12.3

4.6.1. Recommendations

A. Implement usage policies that require explicit management approval to use wireless networks and devices in the CDE. Any unsanctioned wireless should be prevented from connecting to, or detected and removed from CDE as soon as possible.

B. Implement usage policies to require that wireless access is authenticated with user ID and strong password or other authentication item (for example, token). WPA Enterprise supports this requirement. If PSKs are used, then they must be rotated whenever employees that have access to wireless devices leave the organization. In Enterprise mode, individual user access can be enabled/disabled centrally. [See Section 4.4.1 for recommendations on authentication.]

C. For Bluetooth: Verify that the usage policies require that wireless access is authenticated with the proper pairing policy. [See Section 4.4.1 for recommendations on pairing policy.]

D. Include wireless security awareness in training programs for all users of wireless technologies.

E. Communicate wireless usage policies to all users of wireless technologies, and require user acknowledgement that wireless policies are understood and will be adhered to.

5. Industry Documents and External References

The following table shows the documents upon which this document draws its source of reference.

Reference	Location
1. PCI DSS v2.0 and supporting documents	https://www.pcisecuritystandards.org/
2. MasterCard Wireless LANs - Security Risks and Guidelines	http://www.mastercard.com/us/sdp/assets/pdf/wl_entire_manual.pdf
3. Wireless Security Checklist Version 5, Release 2.2	http://iase.disa.mil/stigs/net_perimeter/index.html
4. MasterCard Electronic Commerce Security Architecture Best Practices	http://www.powerpay.biz/docs/risk/MC_best_practices_online.pdf
5. The Center for Internet Security Wireless Networking Benchmark	http://www.cisecurity.org
6. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE Std. 802.11S	http://standards.ieee.org/getieee802/download/802.11-2007.pdf
7. Wi-Fi Alliance	http://www.wi-fi.org/
8. Battered, but not broken: understanding the WPA crack, Glenn Fleishman, Nov, 2008	http://arstechnica.com/articles/paedia/wpa-cracked.ars
9. Ultimate wireless security guide: An introduction to LEAP authentication	http://articles.techrepublic.com.com/5100-10878_11-6148551.html
10. Understanding WEP Weaknesses: Hacking Wireless Networks For Dummies By Kevin Beaver, Peter T. Davis, Devin K. Akin, ISBN: 978-0-7645-9730-5	http://www.dummies.com/WileyCDA/DummiesArticle/Understanding-WEP-Weaknesses.id-3262,subcat-NETWORKING.html
11. ANS X9.112 Wireless Management and Security for the Financial Services Industry	http://www.x9.org
12. NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General	http://csrc.nist.gov/
13. NIST Publication 800-121 Guide to Bluetooth security	
14. NIST SP 800-48, Wireless Network Security: 802.11, Bluetooth and Handheld Devices	
15. NIST Guide to Intrusion Detection and Prevention Systems (IDPS)	

6. Glossary of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access point
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
CCMP	Counter Mode CBC MAC Protocol
CDE	Cardholder data environment
PCI DSS	Payment Card Industry Data Security Standard
EAP	Extensible Authentication Protocol
GPRS	General packet radio service
GSM	Global System for Mobile
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IDF	Intermediary distribution frame
IDS	Intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IPS	Intrusion prevention system
IPSec	Internet Protocol Security
LAN	Local area network
LDAP	Lightweight Directory Access Protocol

Acronym	Definition
MAC	Media Access Control
MIC	Message integrity code
NDS	Netware directory services
OTP	One-time password
PDA	Personal data (Digital) assistant
PoS	Point of sale
PSK	Pre-shared key
QoS	Quality of Service
SIG	Special interest group
SNMP	Simple Network Management Protocol
SOHO	Small office/home office
SSID	Service set identifier
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
URL	Universal resource locator
VLAN	Virtual local area network
WEP	Wired Equivalent Privacy
WLAN	Wireless local area network
WPA	Wi-Fi Protected ACCESS

7. Acknowledgements

The PCI SSC would like to acknowledge the contribution of the Wireless Special Interest Group (SIG) in the preparation of this document. The Wireless SIG consists of representatives from the following organizations:

7safe
ABC Financial Services, Inc
AirDefense, Inc
AirTight Networks
Apriva
AR Technology
ARC Corp
Aruba Networks
Assurant
Bank of America
Canadian Tire
Capita Group
Capital One
Chicos
Cisco Systems, Inc
Citi
The College Board
Colubris Networks
Comsec Global
DB Builder, Inc
DST Output
Expedia Inc
Fishnet Security
Fujitsu US
Harland Clarke Holdings
HP
Hypercom
IBM
Information Risk Management
Ingenico
Innove LLP
Juniper Networks
Limited Brands Inc
Live
Loblaws Companies Ltd
McDonalds Corp
Motorola
Network Frontiers
Nettitude
Nixu
NSS Labs
Palsit
PayPal
Qwest Communications
Rapid7
SecureState
Shell
SonicWall
Spacenet
Sprint
Time Inc
T-Mobile
Transaction Network Services
Tripwire
Tesco UK
VeriFone
Verizon Business
Wyndham Worldwide

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement, and dissemination of the PCI Data Security Standard (DSS), PIN Transaction Security (PTS) Requirements, and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors, and point-of-sale vendors are encouraged to join as Participating Organizations.