

## PCI DSS Wireless Security FAQ



6410 N Business Park Loop Rd.  
Suite E  
Park City, UT 84098  
(435) 615-6711  
[www.aegenis.com](http://www.aegenis.com)

*By Michael Dahn, MSIA, CISSP*

## Table of Contents

Executive Summary .....	1
PCI DSS Overview and Taxonomy .....	2
Taxonomy.....	2
Scope of the PCI DSS .....	3
Compliance vs. Validation .....	3
Compliance vs. Security.....	3
Compensating Controls .....	4
Universally Applicable Wireless Requirements.....	5
PCI DSS Requirement 11.1 Explained .....	5
Frequently Asked Questions Regarding Requirement 11.1 .....	5
Requirements Applicable for In-Scope Wireless Networks.....	7
PCI DSS Requirements Explained.....	7
Frequently Asked Questions Regarding In-Scope Wireless Networks.....	9

## Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) is the foundation for information security requirements within the Payment Card Industry, and is quickly becoming a minimum security baseline for companies around the world. The ability to understand and interpret this standard is essential for companies that wish to adhere to it and properly manage the risk within their organization.

Of the many requirements within the PCI DSS, the Payment Card Industry especially scrutinizes wireless networks because of their wide deployment and potentially serious impact to the security of corporate networks. Unlike other technologies, wireless devices provide attackers a unique attack vector over which to directly compromise Cardholder Data. Only by understanding the industry taxonomy and the specific risks behind wireless technology can one properly mitigate the risk to both their systems and the Cardholder Data they store.

This Frequently Asked Questions (FAQ) document is broken down into two primary sections that distinguish between wireless security requirements that all companies should address and those requirements specific to companies that have in-scope wireless networks.

- Universally Applicable Wireless Requirements: These are requirements that all companies should have in place to protect their wired networks from attacks via rogue access points and other unknown devices using wireless radios. They apply to companies regardless of their use of wireless technology. As a result they are universally applicable to companies that wish to comply with the PCI DSS.
- Requirements Applicable for In-Scope Wireless Networks: These are requirements that all companies who rely on wireless technology should have in place to protect Cardholder Data. They are specific to companies that use wireless technology that is in-scope for PCI DSS compliance. These requirements apply in addition to the aforementioned universally applicable set of requirements.

In addition, this document includes an overview of key terms and definitions used within the context of PCI and are required to properly understand the scoping and security controls surrounding compliance.

The Aegenis Group is uniquely qualified to create this document based on its long experience in the Payment Card Industry and involvement with the PCI DSS standard. The company founders have worked for both Visa Inc. and MasterCard Worldwide where they participated in the training and continued update of the PCI standard. The Aegenis Group members were involved in the development of the original Cardholder Information Security Program (CISP), the precursor to the PCI DSS, and the Payment Application Best Practices (PABP). The team members are former Qualified Security Assessors (QSA) and now train Fortune 500 companies on proper implementation of the standard. In 2007, the Aegenis group trained over 7,000 individuals from more than 500 global companies on the PCI DSS standard.

## PCI DSS Overview and Taxonomy

In 2006, the major card brands, Visa Incorporated, MasterCard Worldwide, American Express, Discover Financial Services, and JCB, collectively created an industry consortium known as the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC is responsible for the management, enhancement, and development of a common industry data security standard, entitled the Payment Card Industry Data Security Standard (PCI DSS).

This set of twelve requirements outlines the minimum security measures for protection against electronic and paper theft of Cardholder Data. In order to discuss the requirements, their scope, how they apply, and potential compensating controls one must first understand a common language with which to discuss each item.

### *Taxonomy*

Understanding how the PCI DSS defines Cardholder and Sensitive Authentication Data is critical to determining the applicability and scope of any PCI DSS effort. The following are relevant definitions that will be used throughout this document when discussing the PCI DSS:

#### *PCI DSS*

The Payment Card Industry Data Security Standard (PCI DSS) is a set of 12 high-level requirements and numerous sub-requirements that define the controls that must be in place to protect Cardholder Data (as defined below). The PCI DSS is endorsed by the five major card brands and adherence is required for any organization that stores, transmits, or processes Cardholder Data.

#### *Payment Card*

Payment Cards are issued by major card brands, such as Visa, and are used to make purchases. Payment Cards include credit, debit, gift, and loyalty cards.

#### *Primary Account Number (PAN)*

The PAN is the 12-16 digit number that is embossed or printed on the front of a Payment Card. This number is unique to a particular cardholder.

#### *Cardholder Data*

Cardholder Data is defined very specifically by the PCI DSS and is the determining factor as to the applicability and scope of the PCI DSS effort. Cardholder Data as defined by the PCI SSC, consists of the Primary Account Number (PAN) alone, and also includes the Cardholder Name, Service Code, and Expiration Date when any of these elements are stored in conjunction with the PAN.

#### *Sensitive Authentication Data*

Sensitive Authentication Data consists of data elements that are transmitted with the initial authorization request in either a card-present or card-not-present transaction. These data elements provide additional authentication of the cardholder. Sensitive Authentication Data consists of the following elements:

- Card Validation Code 2 (CVV2, CVC2, CID, CAV2)
- Track 1 or Track 2 from the Magnetic Stripe
- PIN Blocks

Sensitive Authentication Data may not be retained subsequent to the merchant receiving the initial authorization response message.

### *Cardholder Data Environment*

The Cardholder Data Environment (CDE) is defined as those systems that store, transmit, or process Cardholder Data or any systems that are connected to the CDE without adequate segmentation to limit the access to the CDE and protect Cardholder Data.

### *Scope of the PCI DSS*

The PCI DSS applies to any organization that stores, transmits, or processes Cardholder Data. The scope of PCI DSS is defined as any system comprising the Cardholder Data Environment (CDE), as defined above. This could include, but is not limited to, any network device such as firewall or router, any server or workstation that stores or has access to Cardholder Data, or any application that may interface with such systems and Cardholder Data. Many areas of the corporate network could be included in CDE if they have network access to the CDE.

One of the ways to reduce the scope of PCI DSS is to provide adequate segmentation between the CDE and other corporate systems. Although this document does not outline the nuances behind network segmentation, it does address the concepts behind proper scoping. The definition of “adequate segmentation” is anything that prevents one set of systems from negatively impacting the security of another set of systems, namely those included within the CDE. This segmentation can take the form of network, operating system, application, or operational security controls. The requirements for adequate segmentation will vary between environments and is based on the data present, attack vectors available, and protection mechanisms in place.

### *Compliance vs. Validation*

Compliance with the PCI DSS is mandatory for all companies that store, process, or transmit Cardholder Data. Companies must be in a state of compliance at all times. This means that companies must adhere to each PCI DSS requirement at all times regardless of prior demonstration or documentation of that compliance. Consider compliance analogous to the requirement for a driver to have automobile insurance. The driver is required to have automobile insurance at all times while operating a motor vehicle.

Validation on the other hand is a point-in-time demonstration of compliance, usually to a third party. Validation of compliance with the PCI DSS is not always requested or required. The level and degree of validation may vary based on type of organization, their volume of Payment Card transactions, or other card brand requirements. Continuing the automobile insurance analogy, validation is similar to demonstrating to a police officer, when requested, that you do have automobile insurance.

The types of validation may include preparation of a Report on Compliance (ROC) based on the Security Audit Procedures (SAP) or a Self Assessment Questionnaire (SAQ). These forms of validation mandate verification procedures that are meant to confirm the mitigation of a threat. It is important to remember that although validation happens at a point in time, the act of complying is something that must happen continuously. In the event of a data breach and subsequent forensic investigation, the examiners will validate if the affected company was in compliance with all PCI DSS requirements at the time of the compromise.

### *Compliance vs. Security*

Compliance and security are often erroneously used interchangeably. Compliance can be defined as adherence to a defined set of standards. For example, the PCI DSS is a set of security requirements with

which many members of the Payment Card Industry must comply. There are other compliance standards for other industries. It is important to understand that compliance is a minimum and not a gold standard.

Security is a measure of protection against risk. It can vary from insecure, a low level of protection, to very secure, a high level of protection. Additionally, the determination of the level of security is predicated upon the amount of risk present. Controls should be commensurate with the identified risk.

Compliance, on the other hand, is an objective, static test of adherence to a known standard. If the standard is designed in such a manner as to address some known risks, then the inference derived from a statement of compliance is that a company has achieved some level of security. It is possible however, that security and compliance may diverge. For example, a company may have legal data retention periods longer than those mandated by PCI DSS or may require increased security for systems outside the CDE. Both of these examples are situations where the level of security required is higher than the level of compliance.

### *Compensating Controls*

Achieving compliance should be obtainable regardless of the unique aspects of a corporate environment. Compensating controls take the PCI DSS requirements beyond a simple checklist into a risk based approach towards compliance. If a company cannot directly achieve compliance with the literal wording of a given requirement, based on a legitimate technical or documented business constraint, they can leverage one or more compensating controls. These compensating controls must meet the intent of the original control. In this way a company can leverage additional security controls to meet the intent behind the PCI DSS and achieve compliance.

## Universally Applicable Wireless Requirements

### *PCI DSS Requirement 11.1 Explained*

Although the PCI DSS outlines requirements for securing existing wireless technologies, there are validation requirements that extend beyond the known wireless devices and require monitoring of unknown and potentially dangerous ‘rogue’ devices. A rogue wireless device is an unauthorized wireless device that can allow access to the CDE. PCI DSS requirement 11.1 says companies must “assure the ability to adequately identify and to stop any unauthorized access attempts.” Furthermore, sub-section (b) states that companies should identify unauthorized wireless devices using a wireless analyzer.

Requirement 11.1.b is intended to ensure that companies are aware of their wireless infrastructure and prevent unauthorized wireless access such as rogue access points (APs) or malicious clients. The following questions explain the nuances of how this is implemented within a retail environment.

### *Frequently Asked Questions Regarding Requirement 11.1*

#### **Scanning all of my retail locations sounds difficult. Does PCI really require compliance with the PCI DSS 11.1?**

Yes. The purpose of the requirement is to ensure that unauthorized or rogue wireless devices cannot access the CDE. The goal is to prevent an attacker from using rogue wireless devices to compromise the security of Cardholder Data. It is acceptable to use wireless scanning as defined by the PCI DSS or a preventative control such as a Wireless Intrusion Prevention System (WIPS). Since a rogue device can potentially show up in any location, it is important that all locations are either scanned regularly or that preventative measures are implemented in all locations.

#### **We do not have any wireless deployed. Do we still need to comply with the PCI DSS 11.1 requirement?**

Yes. Although a company may not have purposefully deployed wireless devices, the objective of this requirement is to identify unauthorized or rogue wireless devices. Examples of this can range from a department unwittingly installing an unauthorized wireless access point for convenience to an attacker planting a rogue wireless AP to gain access to the internal network.

#### **We have segmented our wireless network out of PCI scope. Do we still need to perform quarterly wireless scanning for PCI DSS 11.1 compliance?**

Yes. Although adequate network segmentation and other technologies can reduce the CDE scope it does not remove the need to comply with requirement 11.1. The objective of this requirement is to identify unauthorized or rogue wireless devices, such as rogue APs. A rogue device can show up on any network segment including those that are in the CDE.

#### **Our wireless network is on a separate VLAN from our Cardholder Data Environment. Do we still need to perform quarterly wireless scanning for PCI DSS 11.1 compliance?**

Yes. As mentioned previously, compliance with requirement 11.1 is independent from the configuration of sanctioned wireless networks.

#### **There is a firewall between our wireless network and our Cardholder Data Environment. Do we still need to perform quarterly wireless scanning for PCI DSS 11.1 compliance?**

Yes. As mentioned previously, compliance with requirement 11.1 is independent from the configuration of sanctioned wireless networks.

**We are using sophisticated encryption technology to protect our wireless network. Do we still need to perform quarterly wireless scanning for PCI DSS 11.1 compliance?**

Yes. As mentioned previously, compliance with requirement 11.1 is independent from the configuration of sanctioned wireless networks.

**To comply with PCI DSS 11.1, can I choose a sample of a few representative sites for scanning?**

No. A company may not choose to select a sample of sites for compliance. Companies must ensure they scan all sites quarterly to comply with the standard. The company is responsible for ensuring that the CDE is compliant at all times. To be compliant companies must scan their entire CDE with a wireless analyzer at least quarterly. During a PCI DSS assessment, the company or their assessor may choose to validate compliance with 11.1 by choosing a sample of all locations. The PCI SSC leaves sampling, for the purposes of validation, at the discretion of the company or their assessor. As part of the validation, the assessor should check that the company has the appropriate process and technology in place to comply at all locations.

**To comply with PCI DSS 11.1, can I use a wired network scanning tool instead of a wireless analyzer?**

No. To comply with 11.1, a company must mitigate the risk of unauthorized or rogue wireless devices. This is most often achieved by the use of a wireless analyzer. Scanning the wired network for wireless devices may identify some unauthorized wireless devices but may not identify other important wireless attack vectors. The first omission of wired network scanning is that it may miss cleverly hidden and disguised rogue wireless devices that are connected to isolated network segments. Another omission of wired scanning is that it cannot detect rogue wireless clients. A rogue wireless client is any device that has a wireless interface that is not intended to be present in the environment. Although insufficient on their own, wired analysis tools can be very valuable when used in conjunction with wireless analyzers to improve the quality of the scan results.

**To comply with PCI DSS 11.1, may I have technical staff members physically walk through each of my sites with a wireless analyzer instead of automating the process?**

Yes. Although this method is technically possible it is often times operationally tedious, error prone, and costly. Companies can use freely available tools such as NetStumbler or Kismet as wireless analyzers. Using one of these tools, a technician or auditor can physically visit each site and obtain a list of the wireless devices nearby. The technician is then required to manually investigate each device to determine if it allows access to CDE.

**What should the output of the quarterly scan for PCI DSS 11.1 contain?**

Although the PCI DSS standard does not directly state what the output of wireless analyzer should be, it does imply that it should be created, reviewed, and used to mitigate the risk of unauthorized or rogue wireless devices. At a minimum, the list of wireless devices should clearly identify all rogue wireless devices connected to any network that has access to the CDE.

**If I find a rogue wireless device as a result of the wireless scan, am I required to mitigate the threat?**

To comply with the intent of PCI DSS 11.1, companies should immediately remediate the rogue threat and rescan the environment at the earliest possible opportunity. This is similar to other verification requirements within the PCI DSS.

# Requirements Applicable for In-Scope Wireless Networks

## *PCI DSS Requirements Explained*

### **Requirement 4.1.1: Encryption**

The PCI DSS requirement 4.1.1 pertains to the encryption of Cardholder Data over wireless networks. The wording of the requirement can be confusing if one does not understand the intent. The requirement specifically states that companies must encrypt Cardholder Data that traverses wireless networks. There are several ways to accomplish this:

- Secure wireless traffic using WPA/WPA2 - The requirement specifically calls out this method of securing the wireless traffic as optimal. Whenever possible companies should secure the wireless traffic using either of these methods utilizing a TKIP or AES-CCMP cipher.
- Encrypt wireless traffic using IPSEC or SSL/TLS - This approach encrypts the underlying traffic that traverses the wireless network. It does not secure the 802.11 wireless protocol, but it does encrypt the underlying TCP/IP traffic. In doing so, it encrypts the Cardholder Data which is the intent of this requirement.
- Encrypt Cardholder Data at the endpoints - Another option is to encrypt Cardholder Data using the POS unit or application itself. This will protect the PAN and any Sensitive Authentication Data end-to-end as it traverses the wireless network.

Requirement 4.1.1 specifically states that companies should never rely exclusively on Wired Equivalent Privacy (WEP). Industry researchers have shown WEP to be insecure. In recent studies, researchers were capable of cracking WEP in under one minute. This means that companies cannot rely exclusively on WEP because it provides little security. The requirement lists a number of items that should be used to further protect the Cardholder Data in the event a company is currently using WEP. It is not necessary that companies implement each of these as they are simply suggestions for how a company may protect the Cardholder Data when sent over a virtually unprotected network. Any company using WEP must understand that it is inherently insecure and implement one or more of the above mentioned options instead of, or in addition to the use of WEP.

### **Requirement 10.5.4: Logging**

PCI DSS 10.5.4 requires companies store, protect, and review wireless logs just as they would any other audit log event. To understand the intent behind the necessary level of audit log retention and review, one need only look at requirement 10.1 which states “establish a process for linking all access to system components ... to each individual user.” The intent behind audit logging is twofold:

- Retain audit logs for a period of 12 months such that they can facilitate a forensic investigation
- Review audit logs daily to alert administrators of suspicious events

Wireless audit logs can be critical for alerting on suspicious activity if someone is attacking their network. Also, retaining these logs can prove that the exposure of a security breach is limited by quantifying the scope of an attack.

### **Requirement 1.3.8: Firewalls**

The PCI DSS requirement 1.3.8 discusses how companies should protect their wired networks from their sanctioned wireless infrastructure. The requirement calls for firewalls between the wireless networks and the CDE, but this may vary depending on the implementation of wireless security within each company. Certainly if there is no segmentation present and a wireless access point is directly connected to the CDE, a firewall or some other layer of segmentation is required. The question is: what is considered sufficient to meet the intent behind the requirement?

The definition of sufficient segmentation is any that will prevent the systems and people on one network (the wireless network) from negatively impacting the security of Cardholder Data on another network (the CDE). Identifying the specifics behind this can be complex and are very specific to each environment. Companies should evaluate each of the attack vectors and verify that their segmentation, be it with firewalls or alternative technologies, is sufficient to repel an attack of the CDE or connected networks.

#### **Requirement 2.1.1: Changing Default Settings**

The PCI DSS requirement 2.1.1 details the methods used for securing a wireless network by changing the default settings. The requirement specifically calls out many settings that should be changed when permissible. The following is a list of default settings that companies should change:

- Service Set Identifier (SSID)
- SNMP community string
- SSID broadcast

Certainly there are other default settings that companies should change, which may vary based on their specific wireless technology. These may include, but are not limited to:

- Administrative passwords
- Vendor or company identification information
- Audit log settings
- Remote administration methods

The list of settings necessary to secure wireless devices may change between vendors or implementation type, but the intent behind requirement 2.1.1 is to secure devices such that they do not disclose unnecessary information or enable an attacker to access the CDE. It is not required that companies enforce each of the recommended methods for securing a wireless device, but using a secure configuration should protect the wireless infrastructure to attacks that could result in the loss of Cardholder Data.

#### **Requirement 9.1.3: Physical Security**

The PCI DSS requirement 9.1.3 promotes the need for physical security surrounding wireless devices. The focus of this requirement, as with 9.1.2, is on securing publicly accessible or risky devices. For example, one would not put a physical cage around every access point or chain down every handheld device, but one should secure those that are generally accessible to the public or at risk of being lost or stolen.

Although the requirements do not state how to secure wireless devices, there are many ways to implement physical security. Options for securing wireless devices may include physically restricting access to the console interface, preventing the Ethernet cable from being removed, or properly password protecting risky wireless devices. How and when these security measures are leveraged will depend on the individual company and their policy regarding the use of wireless devices.

#### **Requirement 11.4: Intrusion Detection**

The PCI DSS requirement 11.4 mandates the use of intrusion detection technology. This can be leveraged on the host or network, but it must cover and address all networks including those wireless networks. Companies can leverage a variety of technologies to implement this, but should be certain they are identifying attacks against their wireless networks and responding to them as outlined in the corporate incident response plan.

### **Requirement 12.3: Written Policy**

The PCI DSS requirement 12.3 mandates the need for acceptable usage policies and procedures, which include those for wireless devices. The importance here is that companies understand how wireless is to be used within the enterprise environment, how it is to be secured and deployed, and how the company will address incidents as they occur.

Another important aspect of the policy should address how employees can and should use their authorized wireless devices. For example, if an employee receives a laptop they need to understand the acceptable usage responsibilities of the wireless radio. If an employee receives a wireless inventory device they need to understand how to properly protect, access, and store that device.

### *Frequently Asked Questions Regarding In-Scope Wireless Networks*

#### **We have many legacy WEP devices that cannot be upgraded to WPA. What can we do to comply with PCI DSS 1.1 requirement 4.1.1?**

To comply with requirement 4.1.1 companies must encrypt the Cardholder Data and Sensitive Authentication Data as it traverses the wireless network. This encryption cannot be WEP alone. Examples of encryption schemes that can be used in conjunction with WEP are Secure Socket Layer (SSL), Virtual Private Networks (VPNs), or other accepted industry standard encryption mechanisms. Note that WEP key rotation, MAC address filtering, and the use of a 104 / 128 bit WEP keys are not sufficient without the use of an additional encryption mechanism as outlined above.

#### **What are some typical compensating control mechanisms that allow PCI DSS compliant usage of WEP?**

The primary challenge with WEP is that the key can be cracked in a very short period of time – usually a few minutes or less. Compensating controls could include technologies that automatically rotate the key on a per-frame basis, systems that use active defense to prevent WEP key cracking, or other vendor specific technologies that may be applicable to a specific environment.

#### **Although the PCI DSS now provides a way to use WEP and be compliant, should we be preparing to move entirely to WPA/WPA2?**

Yes. WEP is no longer considered secure and the use of WEP alone is not acceptable for compliance with the standard. All companies using WEP should have a migration plan for moving to WPA2 or newer technology.

#### **What type of information for wireless networks do we need to log in order to comply with PCI DSS requirement 10.5.4?**

Companies should maintain appropriate wireless logs with sufficient information to achieve the two goals of alerting on suspicious activity and facilitating a forensic investigation. These logs may include all associated wireless users, the period of time they were connected and active, the amount of data that was received, and the signal strength.

#### **How many days of logs should we maintain to comply with PCI DSS requirement 10.5.4?**

PCI DSS requirement 10.7 states that companies must retain audit logs for at least one year.

#### **Does PCI DSS require us to regularly review wireless logs?**

Yes. PCI DSS requirement 10.6 states that companies must review audit logs at least daily. This does not mean a manual review of each audit log entry and typically involves the use of automated tools that alert on suspicious activity.

**What default settings should be adjusted to comply with 2.1.1?**

At a minimum, companies should work to implement each of the actions outlined for securing wireless devices. This may include: changing the default SSID, disabling the SSID broadcast when possible, changing or disabling SNMP community strings, changing default passwords, utilizing WPA or WPA2 when available, and other security related settings as outlined by the product vendor. The ultimate goal is to secure the wireless device from compromise via known or default settings and configurations.

**Does broadcasting my SSID prohibit compliance with PCI?**

No. As a part of requirement 2.1.1, disabling SSID broadcasting is mentioned; however, this method of securing a wireless network is deprecated. More important than disabling SSID broadcasting is choosing an SSID that does not clearly identify the company or the type of network to which the SSID provides access. For example, do not create an SSID that contains the company's name or business area.

**What does "publicly accessible" mean with regard to wireless access points?**

PCI DSS requirement 9.1.3 discusses restricting physical access to publicly accessible wireless devices. Publicly accessible access points are those that are within the physical reach of individuals when they are within a company's facility. An access point mounted to a wall six feet off the ground is considered publicly accessible. An access point mounted to a ceiling that is eighteen feet high is not generally considered to be publicly accessible.

**What is the best way to physically restrict access to publicly accessible access points?**

Most enterprise-grade access points provide mounting kits that can be locked with a computer lock-and-cable apparatus. When the lock is engaged, the ports on the access point cannot be physically accessed. A would-be intruder could not unplug the Ethernet cable or connect to the console/serial port.

**What is the best way to physically restrict access to my wireless handheld devices?**

By their nature, wireless handheld devices are mobile. Aside from simply removing such devices from the CDE scope, the best way to protect these devices is to track their inventory closely and ensure they are not stolen. Also companies should maintain the integrity of the device by requiring a password prior to viewing sensitive configuration information.

**Do we need to perform intrusion detection on wireless networks?**

Yes. The PCI DSS mandates coverage for wireless devices throughout the standard. Intrusion detection or prevention should cover all networks including traffic from wireless devices.

**What type of wireless usage policies are required for complying with PCI DSS requirement 12.3?**

Although requirement 12.3 does not mandate the technical aspects of wireless security policies it does mandate that companies maintain acceptable use documents for wireless technology. Companies should have written policies that: prohibit rogue wireless devices, require wireless to be disabled on devices that do not require it for operation, prohibit wireless laptops from connecting to the wired and wireless networks at the same time, prohibit employees from connecting to neighboring networks, device appropriate use of hotspots, prohibit employees from connecting to the guest network, and require that pre-shared keys, when in use, are changed at reasonable intervals.

### **About The Aegenis Group, Inc.**

The Aegenis Group is dedicated to helping companies navigate the choppy waters of data security, information risk, and privacy regulation. The Aegenis Group believes that the ability to understand not just the regulatory mandates themselves, but their total impact on the business environment can act as a compelling tool for business enablement. From understanding the ways in which your products and services can protect sensitive data to making the right compliance decisions for your business environment, The Aegenis Group can assist your company in facing the risks associated with an increasingly complex landscape of the business world.

#### **Corporate Headquarters:**

6410 N Business Park Loop Rd.  
Suite E  
Park City, UT 84098  
(435) 615-6711  
[www.aegenis.com](http://www.aegenis.com)  
[info@aegenis.com](mailto:info@aegenis.com)

*© 2007-2008 The Aegenis Group, Inc. All rights reserved Worldwide.*

*The information contained in this document represents the current view of The Aegenis Group, Inc. on the issues discussed herein as of the date of publication. It should not be interpreted as a commitment on the part of The Aegenis Group, Inc. and The Aegenis Group Inc. cannot guarantee the accuracy of the information presented after the date of publication. Specifications and content are subject to change without notice. This white paper is for informational purposes only. THE AEGENIS GROUP, INC MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*The Aegenis Group is a trademark of The Aegenis Group, Inc. Other product or company names mentioned herein may be the trademarks of their respective owners.*

