



**Compliance with the  
Payment Card Industry  
Data Security Standard**  
Meeting the Challenge  
with Symantec Solutions

# Compliance with the Payment Card Industry Data Security Standard

## Meeting the Challenge with Symantec Solutions

### Contents

|                                                                                                                        |    |
|------------------------------------------------------------------------------------------------------------------------|----|
| PCI Data Security Standard Overview . . . . .                                                                          | 3  |
| Scope . . . . .                                                                                                        | 5  |
| PCI Requirement 1 . . . . .                                                                                            | 6  |
| PCI Requirement 2:<br>Do not use vendor-supplied defaults for system passwords and other security parameters . . . . . | 6  |
| PCI Requirement 3 . . . . .                                                                                            | 8  |
| PCI Requirement 4:<br>Encrypt transmission of cardholder and sensitive information across public networks . . . . .    | 8  |
| PCI Requirement 5:<br>Use and regularly update anti-virus software or program . . . . .                                | 9  |
| PCI Requirement 6:<br>Develop and maintain secure systems and applications . . . . .                                   | 10 |
| PCI Requirement 7:<br>Restrict access to data by business need-to-know . . . . .                                       | 11 |
| PCI Requirement 8:<br>Assign a unique ID to each person with computer access . . . . .                                 | 13 |
| PCI Requirement 9 . . . . .                                                                                            | 15 |
| PCI Requirement 10:<br>Track and monitor all access to network resources and cardholder data . . . . .                 | 15 |
| PCI Requirement 11:<br>Regularly test security systems and processes . . . . .                                         | 18 |
| PCI Requirement 12:<br>Maintain a policy that addresses information security for employees and contractors . . . . .   | 19 |

# Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

## Introduction

### CISP/PCI Background

In 1999, Visa USA developed the Cardholder Information Security Program (CISP). The goals of this program were to assure cardholders that their account information was safe, regardless of where it was offered for payment. Originally intended to secure credit card transactions made over the Internet, the CISP was later expanded and mandated in June 2001 to apply to all payment channels, including retail (brick-and-mortar), mail/telephone order and e-commerce.

In order to achieve CISP compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard. The PCI standard is the result of a collaboration between Visa and MasterCard and is designed to create common industry security requirements, incorporating the CISP requirements. Currently, the CISP and PCI Data Security standard has been endorsed by Visa®, MasterCard®, American Express®, Diner's Club®, Discover®, and JCB USA.

If a member, merchant or service provider does not comply with the security requirements or fails to rectify a security issue, they may face fines of up to \$500,000 per incident or restrictions imposed by the credit card companies, including denying their ability to accept or process credit card transactions. The final deadline for compliance with the PCI Data Security standard was June 30, 2005.

### PCI Data Security Standard Overview

#### **The PCI Data Security standard comprises 12 major requirements supported by a set of detailed sub-requirements**

These security requirements apply to all system components. System components are defined as any network component, server or application included in, or connected to, the cardholder data environment. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include but are not limited to Web, database, authentication, Domain Name Service (DNS), mail, proxy and Network Time Protocol (NTP). Applications include all purchased and custom applications, including internal and external Web applications.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

### **The following are the 12 major requirements of the PCI Data Security Standard:**

1. Install and maintain a firewall to protect data.
2. Do NOT use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications (this includes keeping up with the latest security patches).
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

From a high level, these requirements seem fairly easy to implement and maintain. Upon closer review, however, it becomes clear that attaining and maintaining compliance is a much more complex endeavor. We will break down each requirement and show how Symantec solutions can help you "get compliant and stay compliant."

# Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

## Scope

This white paper documents how Symantec products and solutions can address the sections of the PCI Data Security Standard found in the table below. It covers only the sections and subsections that can be addressed using Symantec products and solutions. A full copy of the PCI Data Security standard can be found at:

[http://usa.visa.com/business/accepting\\_visa/ops\\_risk\\_management/cisp.html](http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html)

| PCI Requirement Description     |                                                                                          | Symantec Coverage |  |  |  |  |
|---------------------------------|------------------------------------------------------------------------------------------|-------------------|--|--|--|--|
| Requirement 1                   | Install and maintain a firewall configuration to protect data                            |                   |  |  |  |  |
| Requirement 2 (2.1-2.2)         | Do not use vendor-supplied defaults for system passwords and other security parameters   |                   |  |  |  |  |
| Requirement 3                   | Protect stored data                                                                      |                   |  |  |  |  |
| Requirement 4 (4.1)             | Encrypt transmission of cardholder data and sensitive information across public networks |                   |  |  |  |  |
| Requirement 5 (5.1-5.2)         | Use and regularly update anti-virus software                                             |                   |  |  |  |  |
| Requirement 6 (6.1-6.2)         | Develop and maintain secure systems and applications                                     |                   |  |  |  |  |
| Requirement 7 (7.1-7.2)         | Restrict access to data by business need-to-know                                         |                   |  |  |  |  |
| Requirement 8 (8.1, 8.4-8.5)    | Assign a unique ID to each person with computer access                                   |                   |  |  |  |  |
| Requirement 9                   | Restrict physical access to cardholder data                                              |                   |  |  |  |  |
| Requirement 10 (10.1-10.5,10.7) | Track and monitor all access to network resources and cardholder data                    |                   |  |  |  |  |
| Requirement 11 (11.2)           | Regularly test security systems and processes.                                           |                   |  |  |  |  |

**Figure 1 - Symantec coverage of PCI Requirements**

# Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

## PCI Compliance Challenges

Symantec can assist any organization with complying with the PCI Data Security Standard. In this section, we will select each requirement that our products and solutions address.

### PCI Requirement 1:

Not covered by Symantec solutions

---

### PCI Requirement 2:

#### **Do not use vendor-supplied defaults for system passwords and other security parameters.**

This requirement is based on the fact that one of the easiest vectors for attack from internal or external intruders is using vendor default passwords and default settings to compromise systems. These passwords and settings are generally publicly available and are the simplest way for a hacker to compromise your systems.

#### ***Subsection 2.1***

Always change the vendor-supplied defaults before you install a system on the network (e.g., passwords, SNMP community strings, and elimination of unnecessary accounts).

#### ***The Problem:***

This requirement actually mandates that companies have a set of standards for secure system builds. These builds must be verified prior to implementing the system on the network. Finally, the systems need to be maintained after they have been installed, and tracking this manually can be problematic.

#### ***Symantec Solutions:***

Symantec solutions allow you to generate a thorough configuration report on a machine (server or workstation) prior to putting it into production. This report can be compared with your company's internal standards for secure server builds.

Symantec also provides industry best practices for building and maintaining secure servers and applications. Regardless of platform (Windows®, UNIX®, Novell®) or application (Microsoft®

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

SQL Server, Oracle®, Exchange, or IIS), Symantec solutions will help ensure that every system installed on the network is secure before being put into production.

After the system has been installed, we can then monitor it to help ensure that it stays in compliance with corporate or industry standards. Symantec provides this functionality for both servers AND workstations without requiring an agent on the target machines. Additionally, by leveraging the integration between our solutions and enterprise monitoring tools such as HP® OpenView® or Microsoft® Operations Manager, alerts can be generated and machines remediated to assure continued compliance.

### **Subsection 2.2**

Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best-practices. This subsection includes the following sub-requirements:

- 2.2.1– Implement only one primary function per server (e.g., Web servers, database servers, DNS, etc).
- 2.2.2– Disable all unnecessary and insecure services and protocols.
- 2.2.3– Configure system security parameters to prevent misuse.
- 2.2.4– Remove all unnecessary functionality, such as scripts, drivers, subsystems, file systems.

### **The Problem:**

Keeping track of all the machines in an enterprise, down to the service and subsystem level, is a tedious task, especially in a larger environment. It is even more difficult to monitor services, parameters or protocols, for example, which would make a system prone to misuse. Even with good documentation and change management practices, ensuring that these systems meet this requirement is a tough challenge. This requirement also mandates that IT departments address ALL vulnerabilities and meet industry best practices. Keeping on top of vulnerabilities and best practices can be a full-time job.

There are only two ways to address this problem. The first is the labor and time-intensive way, which is to manually configure each server so that it is secure. The second is to use an

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

automated audit tool that allows every machine in the environment to be continuously monitored for compliance.

### ***Symantec Solutions:***

Symantec solutions can make short work of documenting and monitoring your computing environment. We can gather information down to the service/daemon level to identify exactly what is running on each machine. This simplifies the task of making sure each server performs only a single function. Symantec vulnerability management tools are constantly and automatically updated to identify the latest threats and vulnerabilities in all computing environments. Additionally, Symantec includes reports that are based on industry best practices for building secure servers (i.e., Center for Internet Security Levels 1 and 2), so it is easy to stay up-to-date with maintaining a secure computing environment.

### ***Supported Platforms:***

Windows®, Novell®, UNIX®, IIS, Oracle®, Microsoft® SQL Server

---

### **PCI Requirement 3:**

Not covered by Symantec solutions

---

### **PCI Requirement 4:**

#### **Encrypt transmission of cardholder and sensitive information across public networks.**

Intercepting and diverting data while in transit is a clear and present danger to the security of cardholder data. The best way to secure this sensitive information is to encrypt it prior to transmission over the Internet.

#### ***Subsection 4.1***

Use strong cryptography and encryption techniques (of at least 128-bit) such as Secure Sockets Layer (SSL), PPTP or IPSEC, to safeguard cardholder data during transmission over public networks.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

### ***The Problem:***

It is very important to make sure that all Web servers that have a remote chance of handling cardholder data are utilizing encryption. Getting a handle on which servers are running Web services and how they are configured is a time-consuming, labor-intensive manual process.

### ***Symantec Solutions:***

Symantec solutions allow our customers to quickly identify all Web servers in their computing environment and verify that they have SSL (128-bit) implemented.

### ***Supported Platforms:***

Windows®, Novell®, UNIX®, IIS, Oracle®, Microsoft® SQL Server

---

## **PCI Requirement 5:**

### **Use and regularly update anti-virus software or programs.**

Worms, viruses and spyware pose a major threat to the security of every organization. These malicious programs most commonly enter the network via end-user e-mail activities and Web browsing. It is vital that all systems (servers and workstations) that are connected to the network are running antivirus software with the latest virus definition files installed.

#### ***Subsection 5.1***

Deploy antivirus mechanisms on all systems commonly affected by viruses (e.g., PCs and servers).

#### ***Subsection 5.2***

Ensure that all antivirus mechanisms are current, actively running and capable of generating audit logs.

### ***The Problem:***

Deploying antivirus software in itself is not a big problem. A much larger and more insidious issue is making sure that the antivirus software is up-to-date and actively running on every machine. This task is next to impossible to perform manually, especially in large environments.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

### ***Symantec Solutions:***

Symantec provides solutions that help our customers to quickly and accurately ascertain which machines have antivirus software installed. More importantly, we can determine which virus definition files are being used and whether the antivirus software is actively running. We provide this functionality for both servers and workstations without requiring an agent on the target machines. Additionally, by leveraging the integration between our solutions and enterprise monitoring tools such as HP® OpenView® or Microsoft® Operations Manager, alerts can be generated and machines remediated before they can pose a threat to your computing environment.

### ***Supported Platforms:***

Windows®

---

## **PCI Requirement 6:**

### **Develop and maintain secure systems and applications.**

Security vulnerabilities can be exploited by employees, external hackers, viruses and worms in order to obtain privileged access to systems. Many vulnerabilities can be closed off from exploitation by installing vendor security patches. All systems should have the most current security patches installed to maintain a secure computing environment.

#### ***Subsection 6.1***

Ensure that all system components and software have the latest vendor-supplied security patches. Subsection 6.1.1 requires that all relevant security patches be installed within one month of release.

#### ***Subsection 6.2***

Establish a process to identify newly discovered security vulnerabilities (i.e., subscribe to alert services freely available on the Internet). Update your standards to address new vulnerability issues.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

### ***The Problem:***

Keeping track of the latest security vulnerabilities on all platforms and applications installed in a computing environment is a challenge. Making sure that these security patches are then deployed across ALL systems (servers AND workstations) and applications can be a logistical nightmare. The tight time constraints imposed by this requirement necessitates that some kind of automated solution be used to track and deploy these security patches to maintain compliance with this standard.

### ***Symantec Solutions:***

From a vulnerability tracking perspective, Symantec solutions enable our customers to set up a customized profile for tracking vulnerabilities. Based on the platforms and applications present in the customer environment, we can provide notifications that are filtered, based on their profile.

Symantec has partnered with Shavlik Technologies to provide a best-of-breed patch management and deployment solution. This solution has the capabilities to monitor patch-revision levels on every machine in an environment without the need for an agent. Additionally, we can leverage this architecture to deploy patches in a fast, efficient manner. This solution helps to ensure that your systems (workstations AND servers) and applications (i.e. Microsoft Office suite, and various other applications) are running with the most recent security patches.

### ***Supported Platforms:***

Windows®, Novell®, UNIX®, IIS, Oracle®, Microsoft® SQL Server

---

## **PCI Requirement 7:**

### **Restrict access to data by business need-to-know.**

Restricting access on a need-to-know basis ensures that critical, confidential data can only be accessed by authorized personnel. This restriction reduces the number of users with access to cardholder data, thus reducing the risk of malicious use of this data.

#### ***Subsection 7.1***

Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

### ***Subsection 7.2***

Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

#### ***The Problem:***

The process of identifying and controlling data access permissions across an enterprise is a daunting task. Tracking these controls manually, especially when considering all aspects of the Microsoft security model, is tedious and labor-intensive, even with native tools and utilities. Calculating permissions manually and/or taking shortcuts when attempting to define effective entitlements can lead to false positives OR negatives. There are so many aspects to consider that most enterprises simply accept the risk of not documenting all data access controls, putting them out of compliance with this standard.

#### ***Symantec Solutions:***

Symantec solutions are able to calculate file access permissions in large distributed environments. We have addressed every aspect of the Microsoft security model. File share and NTFS permissions (both directly assigned and inherited), effective group membership (including nested groups), effective local and network access rights, and effective user privileges (Backup, Restore, Take Ownership) are all taken into account when calculating total effective permissions.

This solution can determine what a user has access to, what a group has access to, or what objects have rights to access specific data. Additionally, we can illustrate exactly how these rights were calculated. To ensure that access is only given by a business need-to-know, we have a Web-based interface that can track access permissions by data owner/business unit and allow the data owners to sign off on this access.

We can also report on user access rights and permissions on both the Oracle and SQL Server platforms. Database security is another crucial area in the fight to maintain secure cardholder information.

To ensure that user provisioning is granted according to a business need-to-know, we have an automated solution that handles user provisioning. This provisioning is highly controlled, with permissions granted by business unit or job function. No object is granted any permission without an auditable approval process that ensures all data owners understand and accept responsibility for granting access to this confidential information.

#### ***Supported Platforms:***

Windows®, Active Directory®, Novell®, UNIX®, IIS, Oracle®, Microsoft® SQL Server

# Compliance with the Payment Card Industry Data Security Standard

## Meeting the Challenge with Symantec Solutions

---

### **PCI Requirement 8:**

#### **Assign a unique ID to each person with computer access.**

Assigning a unique ID to every individual ensures that actions taken on critical data and systems can be traced to known and authorized users.

#### ***Subsection 8.1***

Identify all users with a unique username before allowing them to access system components or cardholder data.

#### ***Subsection 8.4***

Encrypt all passwords during transmission and storage, on all system components.

#### ***Subsection 8.5***

Ensure proper user authentication and password management for non-consumer users and administrators, on all system components. This section includes the following sub-requirements:

- 8.5.1– Control the addition, deletion and modification of user IDs, credentials and other identifier objects.
- 8.5.2– Verify user identity before performing password resets.
- 8.5.3– Set first-time passwords to a unique value per user and change immediately after first use.
- 8.5.4– Immediately revoke accesses of terminated users.
- 8.5.5– Remove inactive user accounts at least every 90 days.
- 8.5.6– Enable accounts used by vendors for remote maintenance only during the time needed.
- 8.5.7– Distribute password procedures and policies to all users who have access to cardholder information.
- 8.5.8– Do not use group, shared or generic accounts/passwords.
- 8.5.9– Change user passwords at least every 90 days.
- 8.5.10– Require a minimum password length of at least seven characters.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

- 8.5.11– Use passwords containing both numeric and alphabetic characters.
- 8.5.12– Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- 8.5.13– Limit repeated access attempts by locking out the user ID after not more than six attempts.
- 8.5.14– Set the lockout duration to thirty minutes or until administrator enables the user ID.
- 8.5.15– If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.
- 8.5.16– Authenticate all access to any database containing cardholder information. This includes access by applications, administrators and all other users.

### ***The Problems:***

The two main problems that are addressed with this requirement are user and password management. Both of these issues are problematic because without a set of tools to automate these tasks they are left to skilled personnel (usually help desk administrators). Additionally, it is vital that domain password policies are monitored for any changes that may affect compliance with this requirement. This combined problem has significant labor costs associated with it.

### ***Symantec Solutions:***

Symantec provides a set of tools to automate the entire employee lifecycle. We can handle the creation, provisioning and maintenance of user accounts from hiring to termination. This can be done automatically and securely, in a fully auditable fashion. Business rules and templates can be enforced to handle vendor accounts, terminations and job-change requirements. Prior to implementing this automated lifecycle tool, we have a set of reporting tools that allow you to verify your current environment meets the requirements defined above. It will also proactively monitor these settings to assure continued compliance.

Symantec's Password Self-Service tool ensures that all passwords are only changed after proper authentication. This authentication is accomplished by asking the end-user a set of questions for which only they would know the answer. We can enforce all password strength and complexity requirements, and can perform these resets across various platforms and

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

applications. This application can be accessed from any desktop, even if a user has been locked out and is unable to logon to their workstation.

Finally, Symantec has an offering that will allow you to distribute and track acceptance of password procedures and policies. This tool makes it very simple to provide documented proof of adhering to requirement 8.5.7.

### ***Supported Platforms:***

Windows®, Novell®, UNIX®, IIS, Oracle®, Microsoft® SQL Server (Many other applications can be supported.)

---

### **PCI Requirement 9:**

Not covered by Symantec solutions

---

### **PCI Requirement 10:**

#### **Track and monitor all access to network resources and cardholder data.**

Logging mechanisms and the ability to track user activities are critical for forensic analysis in the event of a problem. Determining the cause or extent of a compromise is next to impossible without a thorough set of system activity logs.

#### ***Subsection 10.1***

Establish a process for linking all access to system components (especially those with administrative privileges such as root) by an individual user.

#### ***Subsection 10.2***

Implement automated audit trails to reconstruct the following events for all system components:

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

- 10.2.1– All individual user accesses to cardholder data.
- 10.2.2– All actions taken by any individual with root or administrative privileges.
- 10.2.3– Access to all audit trails.
- 10.2.4– Invalid logical access attempts.
- 10.2.5– Use of identification and authentication mechanisms.
- 10.2.6– Initialization of the audit logs.
- 10.2.7– Creation and deletion of system-level objects.

### ***Subsection 10.3***

Record at least the following audit trail entries for each event, for all system components:

- 10.3.1– User identification.
- 10.3.2– Type of event.
- 10.3.3– Date and time.
- 10.3.4– Success or failure indication.
- 10.3.5– Origination of event.
- 10.3.6– Identity or name of affected data, system component or resource.

### ***Subsection 10.4***

Synchronize all critical system clocks and times.

### ***Subsection 10.5***

Secure audit trails so they cannot be altered, including the following subset (which Symantec can address):

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

- 10.5.1– Limit viewing of audit trails to those with a job-related need.
- 10.5.2– Protect audit trail files from unauthorized modifications.
- 10.5.3– Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

### ***Subsection 10.6***

Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations. (An audit history usually covers a period of at least one year, with a minimum of 3 months available online.)

### ***The Problems:***

This requirement creates two related problems. The first problem is to make sure that auditing is set up throughout the environment on all systems. This in itself is a highly labor-intensive process, since it requires manual review of all audit settings on all machines in an environment.

The second problem is that once auditing has been enabled, it must be consolidated, reviewed, secured and archived for a defined time period. Without an automated tool, this is also a difficult, labor-intensive task.

### ***Symantec Solutions:***

Symantec is able to verify and configure audit settings across the enterprise on multiple platforms (Windows®, Novell®, and UNIX®) and applications (Microsoft® SQL Server and Oracle®). Additionally, our audit log consolidation tool can gather audit logs across all domain controllers, store them for a defined period of time in a centralized database, and quickly and easily report on all security-related events.

### ***Supported Platforms:***

Windows®, Novell®, UNIX®, IIS, Oracle®, Microsoft® SQL Server  
(Many other applications can be supported.)

**PCI Requirement 11:**

**Regularly test security systems and processes.**

Managing vulnerabilities as they are identified and introduced into an environment is an extremely challenging task. For this reason, it is important that systems, processes and custom software be tested frequently to ensure that security is maintained over time and through changes.

***Subsection 11.2***

Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (i.e., new system component installations, changes in network topology, firewall rule modifications, product upgrades). External vulnerability scans **MUST** be performed by a scan vendor qualified by the payment card industry.

***The Problem:***

It is critical to scan your network for vulnerabilities on a regular basis. While it is required that external vulnerability scans be performed by an outside vendor, it becomes prohibitively expensive to have an outside vendor perform regular internal vulnerability scans.

***Symantec Solutions:***

Symantec has a platform-independent IP scanning tool. Any device connected to the network can be scanned for vulnerabilities on a scheduled or ad hoc basis. This is more than a simple port scanner. It scans for a multitude of vulnerabilities and threats using methods similar to those a hacker might employ. The checks that are packaged with this solution are updated on a regular basis, making it easy to stay on top of the latest threats and vulnerabilities.

Since all external vulnerability scans must be performed by a qualified vendor, Symantec solutions are limited to internal vulnerability scans of the network. This is still a vital part of maintaining a secure computing environment. It is important to note, however, that many external vendors (e.g., Big Four accounting firms) use Symantec solutions for vulnerability scanning.

**PCI Requirement 12:**

**Maintain a policy that addresses information security for employees and contractors.**

A strong security policy is essential for letting employees know what is expected of them. They should all be acutely aware of the sensitivity of cardholder information and know their responsibilities for protecting this information.

***Subsection 12.1***

Establish, publish, maintain and disseminate a security policy that:

- 12.1.1– Addresses all requirements in this specification.
- 12.1.2– Includes an annual process that identifies threats and vulnerabilities, and results in a formal risk assessment.
- 12.1.3– Includes a review at least once a year and updates when the environment changes.

***Subsection 12.2***

Develop daily operational security procedures that are consistent with requirements in this specification (i.e., user account maintenance procedures and log review procedures).

***Subsection 12.3***

Develop usage policies for critical employee-facing technologies, such as modems and wireless, to define proper use of these technologies for all employees and contractors. Ensure that these usage policies require:

- 12.3.1– Explicit management approval.
- 12.3.2– Authentication for use of the technology.
- 12.3.3– A list of all such devices and personnel with access.
- 12.3.4– Labeling of devices with owner, contact information and purpose.
- 12.3.5– Acceptable uses of the technology.
- 12.3.6– Acceptable network locations for these technologies.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

- 12.3.7– A list of company-approved products.
- 12.3.8– Automatic disconnect of modem sessions after a specific period of inactivity.
- 12.3.9– Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.
- 12.3.10– When accessing cardholder data remotely via modem, disable storage of cardholder data onto local hard drives, floppy disks, or other external media. Also, disable cut-and-paste and print functions during remote access.

### ***Subsection 12.4***

Ensure that the security policies and procedures clearly define information security responsibilities for all employees and contractors.

### ***Subsection 12.6***

Make all employees aware of the importance of cardholder information security:

- 12.6.1– Educate employees (i.e., through posters, letters, memos, meetings, and promotions).
- 12.6.2– Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures.

### ***Subsection 12.9***

Implement an incident response plan. Be prepared to respond immediately to a systems breach. This section includes the following subrequirements:

- 12.9.1– Create an incident response plan to be used in the event of system compromise. Ensure that the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing Acquirers and credit card associations).
- 12.9.2– Test the plan at least annually.
- 12.9.3– Designate specific personnel to be available on a 24/7 basis to respond to alerts.
- 12.9.4– Provide appropriate training to staff with security breach response responsibilities.

## Compliance with the Payment Card Industry Data Security Standard Meeting the Challenge with Symantec Solutions

- 12.9.5– Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.
- 12.9.6– Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

### ***The Problem:***

This requirement creates several problems that Symantec can address. It involves the creation and publication of security policies and procedures that cover the responsibilities of employees and contractors. It also requires that these policies and procedures be reviewed and accepted in writing. Finally, it requires the creation and testing of an incident response plan. These policies, procedures and plans require in-depth knowledge of security and technology.

### ***Symantec Solutions:***

Symantec's Web-based solution assists with the creation, dissemination and user acceptance tracking of security policies and procedures. This tool includes templates, quizzes, best practices and the ability to securely store policies in an easy-to-use, Web-based format. It also has the ability to track user acceptance of these policies, for easily proving that employees and contractors have read, understood and accepted their responsibilities as they pertain to securing cardholder data.

Symantec also offers consulting services through our Professional Services organization. This team of highly trained and experienced technical security professionals can assist with compliance gap analysis, implementation and testing of an incident response plan, and creation of a customized set of security policies that map directly to our customers' technical environment and corporate culture.

## About Symantec

Symantec is the world leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, California, Symantec has operations in 40 countries.

More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745-6054.

Symantec Corporation  
World Headquarters  
20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517-8000  
1 (800) 721-3934  
[www.symantec.com](http://www.symantec.com)

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.  
01/06

10526865