NEW BOUNDARY
TECHNOLOGIES®

# New Boundary Technologies®

# The Payment Card Industry (PCI) Security Guide

**New Boundary Technologies**
**PCI Security Configuration Guide**

## CONTENTS

# 1.0 Executive Summary

Recognizing the need for a common set of security requirements and a single validation process, Visa in December 2004 collaborated with MasterCard to create the Payment Card Industry (PCI) Data Security Standard (DSS). Other payment card brands, such as American Express and Discover Card, have also endorsed this Standard within their respective programs and have indicated they will accept on-site assessments performed by a security company approved by Visa. A key component of PCI Data Security Standard implementation success is merchant and service provider compliance.

In September 2006, Visa and American Express, Diner’s Club, Discover, JCB and MasterCard formed the PCI Security Standards Council. The new council has updated the PCI DSS to Version 1.1 with added emphasis on encryption requirements.

The council is an independent body established to govern the security standards for the payments industry. Its goal is to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI Security Standards Council does not manage compliance programs and does not impose any consequences for non-compliance. The PCI DSS Council operates training, testing and certification programs for Qualified Security Assessors (QSA’s) and Approved Scanning Vendors (ASV’s). Each of the five founding payment brands will recognize the QSA’s and ASV’s certified by the PCI Security Standards Council as being qualified to validate compliance to the PCI DSS standards.

The PCI Data Security Standard is designed to help merchants and service providers protect cardholder data wherever it resides in the any of the major credit card vendor payment systems. The PCI Standard program sets forth fundamental security requirements for all merchants and third-party service providers. Validation of these requirements by independent and qualified security companies is also an important required component in the effectiveness of the program. Security Auditors look to the quality, reliability, and consistency of a qualified security program within a merchant’s or service provider’s organization.

This Payment Card Industry (PCI) Security Guide was developed by New Boundary Technologies to provide insight and recommended computer security configurations that can be used by those merchants and service providers who will undergo an onsite review to validate compliance with the PCI Data Security Standard.

In order to meet the compliance requirements of PCI a network administrator needs to develop a PCI Data Security Program. A key part of that program is the development of a security configuration template or security baseline that will “lock down” those computer systems handling cardholder data. In fact Version 1.1, Requirement 2.2 specifically requires vendors to “*add wording to state that configuration standards should be consistent with other standards (NIST, SANS, etc.).”*

To ensure our customers are provided with proven security configuration policies and guidance, Policy Commander contains the Specialized Security-Limited Functionality recommendations from the National Institute of Standards and Technology (NIST) Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.* The complete version of 800-68 is available from NIST at: http://csrc.nist.gov/

Additional information and resources on PCI are available in our PCI Resource Directory available at: http://www.newboundary.com/solutions/pci_guide.htm.

When an IT security configuration template (e.g., hardening or lockdown guide) is applied to a system, in combination with trained system administrators and a sound and effective security program, a substantial reduction in vulnerability exposure can be achieved. In fact, actual testing by the NSA and NIST of these templates on workstations and servers has shown that they will reduce the vulnerabilities on systems by up to 90%.

In the past, applying any security policy was a complex and time-consuming task that required use of numerous complex and separate tools for workstations and servers. Furthermore, once a system was “locked down” with a template or security baseline configuration, it was extremely hard to 1) Detect when a system became “unlocked" or non-compliant and 2) When non-compliance was discovered, it was a manual process to remediate the system and bring it back into compliance. In addition, locking down a workstation without thorough testing can cause unexpected interruptions in availability of applications and network resources. This can lead to productivity losses throughout the organization as end-users become unable to access mission critical applications or network resources. For these reasons and others, network administrators tended to avoid applying security templates to their systems and thus missed an opportunity to eliminate up to 90% of their system vulnerabilities.

To address the complexity of customizing, deploying, managing and maintaining security configurations and policies on desktops and servers, New Boundary Technologies developed Policy Commander™. Policy Commander is a *single security policy management solution* that contains scores of security policies that can be applied to both workstations and servers. It is no longer necessary to learn how to use separate tools and scripting languages for different versions of Windows workstations and servers. To further simplify the process of testing and applying the NIST Security Template, Policy Commander has reduced the numerous individual security settings contained in the NIST templates to a smaller, more manageable collection of security policies. Thus from a central console and database, Policy Commander can quickly deploy a complete Microsoft, NSA or NIST template or a single policy to one or all of your systems. Policy Commander then will continuously monitor the state of computers and security policies, notify users of any instances of non-compliance, and automatically remediate those non-compliant computers and security policies. Policy Commander is a solution that significantly reduces the complexity, time and effort to create, modify, test, deploy, monitor and enforce any security policy on any Windows-based server or workstation located anywhere in you network worldwide.

To see how Policy Commander can help you meet the PCI Data Security Standard, see Appendix A. Table 1 provides an overview of the six major security categories that are required to meet the PCI Security Standard. Table 2 outlines the specific PCI DSS requirements that Policy Commander supports. To view the complete PCI DSS see the PCI Security Standards Council web site. https://www.pcisecuritystandards.org/tech/index.htm

Appendices B and C provides lists of the New Boundary Technologies PCI Security Policy Library policies for workstations and servers.

To download a full Policy Commander evaluation version please visit the New Boundary website at: http://www.newboundary.com/products/policycommander/index.htm.

# 2.0 The PCI Data Security Standard

## 2.1 WHAT IS PCI?

Unlike Congressionally mandated laws such as HIPAA, SOX and GLBA, PCI is not a federal law. It is a private security standard that members, merchants and service providers must follow pursuant to their contracts with the credit card companies such as Visa, MasterCard, and American Express, etc. Although PCI is not a law, it is enforceable by the credit card companies through contractual penalties or sanctions that include revocation of the company's right to accept or process credit card transactions.

## 2.2 WHOM DOES PCI AFFECT?

PCI applies to all members, merchants and service providers that store, process or transmit cardholder data, whether that data is received in a point of sale, phone, e-commerce or other type of transaction. It applies to all system components, which PCI defines as, "any network component, server, or application included in, or connected to, the cardholder data environment."

The PCI standard is made up of a set of twelve individual compliance requirements (each of which includes more detailed compliance steps), organized around six primary goals, all of which add up to a comprehensive information security program for protecting credit card numbers and other sensitive cardholder data from loss or compromise.

In addition to the compliance requirements, PCI also contains ongoing validation requirements. These requirements differ somewhat from one credit card company to another, but the most comprehensive requirements (Visa and MasterCard) include three levels of validation: (1) an on-site security audit; (2) a self assessment questionnaire, and; (3) a network scan. The level of validation required, and the frequency of validation efforts, depends upon the rating assigned to the merchant or service provider under PCI, which is based on risk and transaction or account volume.

## 2.3 WHEN DO YOU HAVE TO COMPLY BY?

All merchants and service providers that handle, transmit, store or process information concerning any of these cards, or related card data, are required to be compliant with PCI as of June 30, 2005. Transition to the Version 1.1 is required by December 2006.

## 2.4 WHAT HAPPENS IF YOU DON'T COMPLY BY THEN?

The PCI program also includes monetary penalties and other contractual sanctions for failure to meet its requirements. For example, under the Visa PCI program, members can be fined up to $500,000 per incident if any merchant or service provider that is not PCI-compliant is compromised. Visa members who fail to immediately notify Visa of a suspected or known loss or theft of transaction information may be fined $100,000 per incident, plus additional fines if a PCI violation presents immediate and substantial risks to Visa and its members.

The bigger penalty is that failure to meet PCI can also result in suspension or revocation of a company's right to accept or process credit card transactions. Of course, loss of reputation and potential business is also a motivation to comply.

## 2.5 KEY SECTIONS THAT PERTAIN TO SYSTEM SECURITY

The PCI compliance requirements consist of twelve major requirements organized into six primary categories.

**Category 1: Build and maintain a secure network**

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

**Category 2: Protect Cardholder Data**

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

**Category 3: Maintain a vulnerability management program**

5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

**Category 4: Implement strong access control measures**

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

**Category 5: Regularly monitor and test networks**

10. Track and monitor all access network resources and cardholder data
11. Regularly test security systems and processes

**Category 6: Maintain an information security policy**

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

**Below is a quick summary of new changes contained in Version 1.1 dated September 2006:**

**2.2:** Added wording to state that configuration standards should be consistent with other standards (NIST, SANS, etc.).

**2.4:** Added hosting provider requirement and Appendix A

**3.4.2:** Added information about how disk encryption should be implemented, if used.

**5.1.1:** New requirement that malicious software, such as spyware and adware, are included in anti-virus software capabilities.

**6.6:** 1. Added requirement for application code review or application firewall.
2. Added note that this is considered a best practice until June 30, 2008, after which it will be a requirement.

**12.10:** Added requirement for a policy to manage connected entities, including maintaining a list, implementing appropriate due diligence, ensuring connected entities are PCI DSS compliant, and having an established process to connect and disconnect entities.

**Appendix A:** Added Appendix A – PCI DSS Applicability for Hosting Providers. Establishes requirements for providers that host merchant and service provider clients.

**Appendix B:** Added Appendix B – Compensating Controls. Defines compensating controls in general and discusses compensating controls when stored cardholder data cannot be rendered unreadable.

## 2.6 POLICY COMMANDER IN PCI

The above categories essentially make up a comprehensive PCI Data Security Program for protecting credit card numbers and other sensitive cardholder data from loss or compromise.

The need to have a PCI Data Security Program or Plan is a common element across all regulatory requirements. Policy Commander plays a key role in a PCI environment, as it does today in HIPAA, GLBA and SOX, by allowing an administrator to lock down and maintain the security configuration of workstations and servers.

With respect to the twelve specific PCI Requirements, Policy Commander directly addresses the following:

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

**Requirement 3:** Protect stored cardholder data.

**Requirement 6:** Develop and maintain secure systems and applications.

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

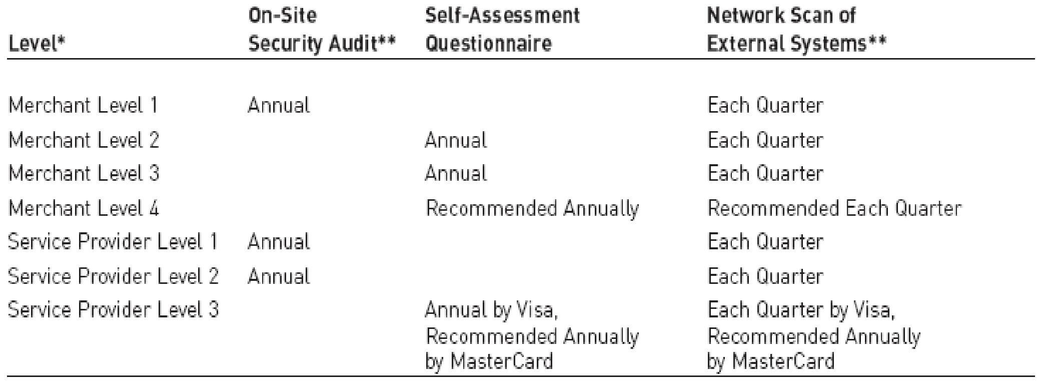
**Requirement 10:** Track and monitor access network resources and cardholder data.

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

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

This Guides Appendix A provides specific details on how Policy Commander helps meet the above requirements. Policy Commander helps set and maintain a secure environment for merchant and service providers who have to meet the PCI security requirements.

## 2.7 VALIDATION REQUIREMNTS: Maintaining and Demonstrating Compliance



| Level* | On-Site Security Audit** | Self-Assessment Questionnaire | Network Scan of External Systems** |
|---|---|---|---|
| Merchant Level 1 | Annual | | Each Quarter |
| Merchant Level 2 | | Annual | Each Quarter |
| Merchant Level 3 | | Annual | Each Quarter |
| Merchant Level 4 | | Recommended Annually | Recommended Each Quarter |
| Service Provider Level 1 | Annual | | Each Quarter |
| Service Provider Level 2 | Annual | | Each Quarter |
| Service Provider Level 3 | | Annual by Visa, Recommended Annually by MasterCard | Each Quarter by Visa, Recommended Annually by MasterCard |

•**Merchant Level 1:** Any merchant (a) processing over 6,000,000 transactions per year, or, (b) that has suffered a breach resulting in account data compromise, or (c) that Visa or MasterCard determine should be Level 1, or (d) that is classified as Level 1 by any other payment card brand.

•**Merchant Level 2:** Any merchant processing 150,000 to 6,000,000 e-commerce transactions per year.

•**Merchant Level 3:** Any merchant processing 20,000 to 150,000 e-commerce transactions per year.

•**Merchant Level 4:** Any merchant not in Level 1, 2 or 3.

•**Service Provider Level 1**: Member Visa or MasterCard processor, or a payment gateway.

•**Service Provider Level 2:** Any Service Provider not in Level 1 that stores, processes or transmits over 1,000,000 transactions or accounts per year.

•**Service Provider Level 3:** Any Service Provider not in Level 1 that stores, processes or transmits less than 1,000,000 transactions or accounts per year.

*Levels are based on volume and/or risk

**On-Site Security Audits and Network Scans must be performed by third party vendors who have been certified by the credit card company.

# 3.0 New Boundary Technologies PCI Security Guide

The purpose of this guide is to provide network administrators with insight on how Policy Commander plays an integral part in applying security configuration policies that will “lock down” Windows XP workstations and Windows servers handling card holder data. The NIST Specialized Security-Limited Functionality template modifies several key areas of a Windows XP system, including password policy, account lockout policy, auditing policy, user rights assignment, system security options, event log policy, system service settings, and file permissions. The template is based on security templates previously developed by the National Security Agency (NSA), Defense Information Systems Agency (DISA), and Microsoft. Most of the settings in the template represent consensus recommendations as proposed by various security experts from the Center for Internet Security (CIS), DISA, NSA, Microsoft, and NIST.

While NIST has developed different template settings for use in Small Office/Home Office (SOHO), Legacy, Enterprise and High Security environments, NIST has recommended that any company that has to comply with any of the federal regulatory requirements should look at using the XP Specialized Security-Limited Functionality template discussed in this guide. Likewise, for the PCI requirements, New Boundary Technologies recommends that any systems (desktops or servers) that will handle sensitive card holder data use or be migrated to the Windows XP operating system. This will not only provide the highest level of security but also significantly ease the task of testing, applying and maintaining the Specialized Security-Limited Functionality template for Windows XP.

## 3.1 High Security Environment

A high security environment is any environment, networked or standalone, which is at high risk of attack or data exposure. This environment encompasses computers that contain highly confidential information (e.g., personnel records, medical records, financial information) and perform vital organizational functions (e.g., accounting, payroll and credit card processing, etc). These computers might be targeted by external parties for exploitation, but also might be targeted by trusted parties inside the organization.

A high security environment could be a subset of a SOHO or Enterprise environment. For example, three desktops or a server in an enterprise environment that hold confidential customer information could be thought of as a high security environment within an enterprise environment. In addition, a laptop used by a mobile worker might be a high security environment within a SOHO environment. A high security environment might also be a self-contained environment outside any other environment: for instance, a government security installation dealing in sensitive data.

Systems in high security environments face threats from both insiders and external parties. Because of the risks and possible consequences of a compromise in a high security environment, it usually is the most restrictive and secure configuration. The suggested configuration provides the greatest protection at the expense of ease of use, functionality, and remote system management. In a high security environment, this guide is targeted at experienced security specialists and seasoned system administrators who understand the impact of implementing these strict requirements.

## 3.2 Best Practices for Analysis and Testing of Security Policies

Although the NIST security settings have undergone considerable testing and are recommended for companies dealing with sensitive information, every system and environment is unique, so system administrators should perform their own testing. The development of the NIST Windows XP Specialized Security-Limited Functionality Template was driven by the need to create a more secure Windows XP workstation configuration. Because some settings in the templates may reduce the functionality or usability of the system, it is not recommended that the complete template be used as a baseline security configuration. Specific settings in the templates should be modified as needed so that the settings conform to local policies and support required system functionality.  New Boundary Technologies strongly recommends that organizations fully test the PCI policies contained in Policy Commander on representative systems before widespread deployment. Some settings may inadvertently interfere with applications, particularly legacy applications that may require a less restrictive security profile.

NBT recommends the following steps be taken to test the policies:

**1) Analyze:** Conduct a risk assessment of the assets in your network that will handle card holder data. Use Policy Commander as part of the risk assessment to compare the current security policies of the local workstation/servers to the policies required to meet the PCI security requirements.

**2) Test:** When new security settings or policies are applied, they can interfere with the operation of existing software applications and other operations on the target computers. We strongly recommend testing each new policy thoroughly in the test environment before moving it to the production environment. Our recommended testing methodology includes the following steps:

- System administrators build their systems from a clean formatted state to begin the process of securing Windows XP workstations and Windows 2003 Server.
- System administrators should perform the installation and test process on a secure network segment or off the organization's network until the security configuration is completed.
- All patches, service packs, hotfixes and rollups for XP/Server 2003 should be applied.
- All desktop or server applications should be installed, operational and have all upgrades/patches applied.
- Strong passwords should be set for all accounts.

**3) Assign:** Use Policy Commander to install the NIST policy modules in the test mode.

In the past, network administrators would have to apply the entire template and then spend hours troubleshooting the dozens of settings to see which ones caused a problem on the test workstation. By reducing the number of settings to a small collection of key policies, network administrators now can individually apply each policy, modify it as necessary, and then add the next policy. This will significantly decrease the time required to test and configure the PCI security configuration that best fits your environment.

The NBT PCI security policies are organized based on the nine categories identified by NIST. Those categories are:

1) Account Policies
2) Local Policies
3) Event Log Policies
4) Restricted Groups
5) System Services
6) File Permissions
7) Registry Permissions
8) Registry Values
9) File and Registry Auditing

Appendix B provides an overview of these nine categories and which New Boundary Technologies PCI Security Policies are in each category. Appendix C is an overview of the Windows Server security policies contained in Policy Commander that can used to lock down the security configuration of servers based on their role.

**4) Enforce:** Save final security configuration baseline, use Policy Commander to organize your key PCI workstations and servers, and then deploy the PCI security configuration baseline. New Boundary recommends that the automatic enforcement feature be utilized to ensure complete 24x7 enforcement of the PCI security configuration.

For a complete overview of how Policy Commander works and to download the 30 day trial version, visit the New Boundary Technologies website at: *http://www.newboundary.com/products/policycommander/index.htm.*

## 4.0 Summary of Recommendations

- Protect each system based on the potential impact to the system of a loss of confidentiality, integrity, or availability.
- Reduce the opportunities that attackers have to breach a system by limiting functionality according to the principle of least privilege and resolving security weaknesses.
- Select PCI security controls that provide a reasonably secure solution while supporting the functionality and usability that users require.

- Use multiple layers of security so that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system.
- Conduct risk assessments to identify threats against systems and determine the effectiveness of existing security controls in counteracting the threats. Perform risk mitigation to decide what additional measures (if any) should be implemented.
- Document procedures for implementing and maintaining PCI security controls. Maintain other security-related policies and documentation that affect the configuration, maintenance, and usage of systems and applications, such as acceptable use policy, configuration management policy, and IT contingency plans.
- Test all PCI security controls, including the settings in the NIST security templates, to determine what impact they have on system security, functionality, and usability. Take appropriate steps to address any significant issues.
- Monitor and maintain systems on a regular basis so that security issues can be identified and mitigated promptly. Actions include acquiring and installing software updates, monitoring event logs, providing remote system administration and assistance, monitoring changes to OS and software settings, protecting and sanitizing media, responding promptly to suspected incidents, performing vulnerability assessments, disabling and deleting unused user accounts, and maintaining hardware.

# # #

# Appendix A

## PCI Security Category and Requirements

Table 1 provides a summary of the PCI Security Categories and the PCI Requirements. Table 2 highlights the specific PCI DSS requirements that Policy Commander supports. The requirements below are from the PCI Security Standards Council, PCI DDS version 1.1 September 2006. The complete PCI DDS can be downloaded from PCI Security Standards Council at https://www.pcisecuritystandards.org/tech/index.htm. The PCI DSS is your starting point for the development of a final PCI Data Security Program tailored for your particular company's needs and requirements. In support of PCI DSS Requirement 2.2, New Boundary also suggests obtaining the National Institute of Standards and Technology (NIST) publication Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.* The complete version of 800-68 is available from NIST at: http://csrc.nist.gov/ .

**Table 1**

| PCI Category | PCI Requirement |
|---|---|
| **1.0 Build and Maintain a Secure Network** | **Requirement 1: Install and maintain a firewall configuration to protect cardholder data** |
| | **Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.** |
| **2.0 Protect Cardholder Data** | **Requirement 3: Protect Stored Cardholder Data.** |
| | **Requirement 4: Encrypt transmission of cardholder data across open, public networks** |
| **3.0 Maintain a Vulnerability Management Program** | **Requirement 5: Use and regularly update anti-virus software or programs.** |
| | **Requirement 6: Develop and maintain secure systems and applications.** |
| **4.0 Implement Strong Access Control Measures** | **Requirement 7: Restrict access to cardholder data by business need-to-know.** |

| | |
|---|---|
| | **Requirement 8: Assign a unique ID to each person with computer access.** |
| | **Requirement 9: Restrict physical access to cardholder data.** |
| **5.0 Regularly Monitor and Test Networks** | **Requirement 10: Track and monitor all access to network resources and cardholder data.** |
| | **Requirement 11: Regularly test security systems and processes.** |
| **6.0 Maintain an Information Security Policy** | **Requirement 12: Maintain a policy that addresses information security for employees and contractors.** |

**Table 2**

**Category 1**

**Build and Maintain a Secure Network**

| PCI Requirements 1&2 | Description | Policy Commander Capabilities |
|---|---|---|
| **Pre-Requirements** | **Risk Analysis**: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic card holder data. | Use Policy Commander to assess current security policy configuration and risk on workstations and servers. |
| | **Risk Management Plan:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Requirements 1 through 12 below: | Use Policy Commander to apply the Industry Best Practice security policies based on the NIST Security Templates in NIST Special Publication 800-68. |
| **Requirement 1.0** | **Install and Maintain a Firewall Configuration to protect cardholder data.**<br>*Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.* | |
| **Rqt 1.1** | **Establish firewall configuration standards that include:** | |
| **1.1.2** | A current network diagram with all connections to cardholder data, including any wireless networks. | Use Policy Commander to identify all workstations and servers that handle card holder data. |
| **1.1.4** | Description of groups, roles, and responsibilities for logical management of network components. | Use Policy Commander to group computers based on their role in handling card holder data. |

| | | |
|---|---|---|
| **1.1.5** | Documented list of services/ports necessary for business. | Use Policy Commander to identify all services running on computers that handle card holder data. |
| **1.3.9** | Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. | Use Policy Commander to identify all PC's with approved firewall software installed and operational. You can also use Policy Commander to install the correct firewall software or remove outdated versions. |
| **Requirement 2.0** | **Do not use vendor-supplied defaults for system passwords and other security parameters.**<br>*(Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information).* | |
| **Rqt 2.2** | Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS). | Use Policy Commander to develop, install and automatically maintain a security configuration baseline that addresses all known security vulnerabilities and industry best practices. |
| **2.2.1** | Implement only one primary function per server (for example web servers, database servers, and DNS should be implemented on separate servers). | Use Policy Commander to establish the security baseline for servers with one primary function. |
| **2.2.2** | Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function). | Use Policy Commander to automatically disable all unnecessary and insecure services and protocols not directly needed to perform the devices' specified function. |
| **2.2.3** | Configure system security parameters to prevent misuse. | Use Policy Commander to set and automatically configure all systems security parameters to prevent misuse. |
| **2.2.4** | Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | Use Policy Commander to automatically remove all unnecessary functionality, such as scripts, drivers, features, |

| | | |
|---|---|---|
| | | subsystems, file systems (e.g., unnecessary web servers). |
| **Rqt 2.3** | Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. | All Policy Commander communications between the server and client are fully encrypted. |
| **Rqt 2.4** | Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers." | Hosting providers can use Policy Commander as outlined in this guide to meet PCI DSS requirements. |

| **Category 2**<br>**Protect Card Holder Data** | | |
|---|---|---|
| **PCI Requirement 3** | **Description** | **Policy Commander** |
| **Requirement 3.0** | **Protect Stored Data**<br>*Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.* | Policy Commander contains a policy that can restrict access to files or folders that contain card holder data to only those with authorized access. |
| **Rqt 3.4** | Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:<br>•Strong one-way hash functions (hashed indexes)<br>•Truncation<br>•Index tokens and pads, (pads must be securely stored)<br>•Strong cryptography with associated key management processes and | Policy Commander contains a policy that can restrict access to files or folders that contain card holder data to only those with authorized access. |

| | | |
|---|---|---|
| | procedures.<br>The MINIMUM account information that needs to be rendered unreadable is the PAN. | |
| **Rqt 3.5** | Protect encryption keys against both disclosure and misuse: | |
| **3.5.2** | Store keys securely in the fewest possible locations and forms. | Policy Commander can create a policy that can restrict access to files or folders that contain encryption keys to only those with authorized access. |

| **Category 3**<br>**Maintain a Vulnerability Management Program** | | |
|---|---|---|
| **PCI Requirements 5 & 6** | **Description** | **Policy Commander** |
| **Requirement 5.0** | **Use and regularly update Anti-Virus software or programs.**<br>*Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.* | |
| **Rqt 5.1.1** | Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware. | With Policy Commander you can create policies that will automatically prevent the installation of persistent Spyware or will automatically detect and remove Spyware if installed. |
| **Rqt 5.2** | Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs. | With Policy Commander you can create a policy that checks to see if the approved corporate Anti-Virus version is installed. |
| **Requirement 6.0** | **Develop and Maintain Secure Systems and Applications.**<br>*Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently* | |

| | | |
|---|---|---|
| | *released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.* | |
| **6.1.1** | Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release. | Policy Commander can create policies to check and maintain the current patch posture of computers. Policy Commander can also be used to automatically re-install patches on computers that become unpatched. |
| **Rqt 6.2** | Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues. | Policy Commander is automatically subscribed to the New Boundary Policy Library where new policies are posted to counter new and emerging vulnerabilities. All policies can be downloaded by customers. |

| **Category 4**<br>**Maintain a Vulnerability Management Program** | | |
|---|---|---|
| **PCI Requirements 7, 8 and 9** | **Description** | **Policy Commander** |
| **Requirement 7.0** | **Restrict access to data by business need-to-know.**<br>*This requirement ensures critical data can only be accessed by authorized personnel.* | . |
| **Rqt7.1** | Limit access to computing resources and cardholder information to only those individuals whose job requires such access. | Policy Commander can restrict access to workstations and servers to only authorized workforce members. |

| | | |
|---|---|---|
| **Rqt 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. | Policy Commander can restrict access to workstations and servers with multiple users to only authorized workforce members and deny access to all others. |
| **Requirement 8:** | **Assign a unique ID to each person with computer access.**<br>*Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.* | |
| **Rqt 8.1** | Identify all users with a unique username before allowing them to access system components or cardholder data. | Policy Commander can restrict access to workstations and servers to users with unique user names. |
| **Rqt 8.3** | Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates. | Use Policy Commander in the DMZ as a Secure Access Gateway for mobile or remote users. Use the Policy Editor to create access policies that will be checked and remediated on all user systems before they are allowed access to the internal network. Use a policy to check to see if the correct version of the VPN client is installed. |
| **Rqt 8.5** | Ensure proper user authentication and password management for non-consumer users and administrators, for all system components as follows: | |
| **8.5.13** | Limit repeated access attempts by locking out the user ID after not more than six attempts. | With Policy Commander you can create a policy that can automatically lock out a user after not more than 6 attempts. |
| **8.5.15** | If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal. | Policy Commander contains a policy that can be set to automatically log off a user after a set time limit. |
| **8.5.16** | Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users. | With Policy Commander you can create a File/Folder Access policy to help verify access to files or folders containing card holder data.<br>This type of policy can also ensure that the information is not improperly modified without detection. |

| | | |
|---|---|---|
| **Requirement 9** | **Restrict physical access to cardholder data.**<br>*Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.* | |
| **Rqt 9.7** | Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data: | Policy Commander contains policies that will prevent the attachment and/or use of portable USB storage devices. |
| **Rqt 9.9** | Maintain strict control over the storage and accessibility of media that contains cardholder data: | Policy Commander contains policies that will prevent the attachment and/or use of portable USB storage devices. |

| **Category 5**<br>**Regularly Monitor and Test Networks** | | |
|---|---|---|
| **PCI Requirements 10 & 11** | **Description** | **Policy Commander** |
| **Requirement 10.0** | **Track and monitor all access to network resources and cardholder data**<br>*Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.* | Policy Commander will automatically identify, respond and correct suspected and known security policy incidents.<br>Policy Commander also maintains a printable record of any action, activity, or assessment conducted on the security configuration established by the administrator. This record can be provided to any PCI auditor. |
| **Rqt 10.6** | Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).<br>*Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.* | Policy Commander will alert you and remediate a computer when an out of compliance condition occurs and generate audit log files for review. |

|  |  |  |
|---|---|---|
| **Rqt 10.7** | Retain audit trail history for at least one year, with a minimum of three months online availability. | Policy Commander generates audit log files for review by auditors |
| **Requirement 11** | **Regularly test security systems and processes.**<br>*Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.* |  |
| **Rqt 11.1** | Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use. | Policy Commander provides real time monitoring and management of the established security policy baseline on all computers. |
| **Rqt 11.2** | Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).<br>*Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.* | Applying the Policy Commander PCI Policy Library will reduce system vulnerabilities by over 90% and significantly reduce the vulnerabilities found by a vulnerability scanner. |
| **Rqt 11.3** | Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include: Network-layer penetration tests and Application-layer penetration tests. | Results from penetration testing should be reviewed to see if Policy Commander can be used to create new policies to prevent discovered vulnerabilities. |
| **Rqt 11.4** | Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date. | Results from intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems should be reviewed to see if Policy Commander can be used to create new policies to prevent discovered vulnerabilities. |

| | | |
|---|---|---|
| **Rqt 11.5** | Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.<br>*Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).* | With Policy Commander you can create File/Folder Access policies that will automatically prevent unauthorized modification of critical system or content files or folders containing card holder data. |

| **Category 6**<br>**Maintain an Information Security Policy** | | |
|---|---|---|
| **PCI Requirements 12** | **Description** | **Policy Commander** |
| **Requirement 12.0** | **Maintain a policy that addresses information security for employees and contractors.**<br>*A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.* | Policy Commander will translate your written PCI security policies for computers into deployable policies that will be automatically monitored and enforced on your computers 24x7.<br>. |
| **Rqt 12.1** | Establish, publish, maintain, and disseminate a security policy that accomplishes the following: | Use Policy Commander to apply the PCI Policy Library based on Visa's Payment Card Industry Security Audit Procedures, version 1.0 January 2005 and on the National Institute of Standards and Technology (NIST) publication Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist* |

| | | |
|---|---|---|
| **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 | Policy Commander is a key solution that continuously and automatically prevents security policy breaches from threats and vulnerabilities. |
| **12.3.10** | When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access. | Policy Commander contains policies that will prevent the attachment and/or use of portable USB storage devices. |
| **Rqt 12.5** | Assign to an individual or team the following information security management responsibilities: | |
| **12.5.1** | Establish, document, and distribute security policies and procedures. | Policy Commander will establish, document, distribute and automatically enforce security policies to individual computers in your network. |
| **12.5.2** | Monitor and analyze security alerts and information, and distribute to appropriate personnel. | Policy Commander will automatically identify, respond and correct suspected and known security policy incidents. Policy Commander will document/log security incidents and provide full reports for audits. |
| **12.5.3** | Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | Policy Commander will document/log security incidents and provide full reports for audits. |
| **Rqt 12.8** | If cardholder data is shared with service providers, then contractually the following is required:<br>12.8.1 Service providers must adhere to the PCI DSS requirements<br>12.8.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses. | A Payment Card Industry service provider can use Policy Commander to implement the same security policies as the covered entity.<br>Policy Commander can also be used by the covered entity as a Remote Access Gateway to enforce selected security policies and configurations on the third party workstations requesting access to the network. |

| | | |
|---|---|---|
| **Rqt 12.9** | Implement an incident response plan. Be prepared to respond immediately to a system breach. | |
| **12.9.6** | Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | Policy Commander's Policy Editor provides the ability to author new policies to adjust to any lessons learned and to incorporate any changes to the incident response plan. |
| **12.10** | All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following: | A Payment Card Industry service provider can use Policy Commander to implement the same security policies as the covered entity. |
| **12.10.3** | Ensure the entity is PCI DSS compliant | A Payment Card Industry service provider can use Policy Commander to ensure PCI DSS compliance. |

# Appendix B

## New Boundary Technologies PCI Workstation Template Settings

This table describes the **Workstation** security policies contained in the New Boundary Technologies PCI Security Policy Library. These policies are organized into nine key security categories based on the National Institute of Standards and Technology (NIST) Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.*

Category 9 contains custom policies developed by New Boundary Technologies to meet other PCI security requirements.

| Security Categories | Policy Commander Policies |
|---|---|
| 1.0 Account Policies | • Harden account lockout settings |
| 2.0 Local Policies<br>2.1 Audit Policies<br>2.2 User Rights Assignment<br>2.3 Security Options | • Control the System Audit Policy settings<br>• Harden the User Rights Assignment settings<br>• Disable the Guest Account<br>• Limit local account use of blank passwords to console only<br>• Harden Device settings<br>• Harden Domain Member settings<br>• Harden Interactive Logon settings<br>• Harden Microsoft network server settings<br>• Harden network access settings<br>• Harden network security settings<br>• Harden Recovery Console settings<br>• Harden Shutdown settings<br>• Enforce FIPS Certified Cryptography<br>• Harden System Objects settings<br>• Shut down immediately if unable to log security audits<br>• Disallow anonymous SID_Name translation<br>• Force logoff when logon hours expire |
| 3.0 Event Log Policies | • Control Event Log settings |
| 4.0 Restricted Groups | • Remove all users from the Remote Desktop Users and Power Users groups. |
| 5.0 System Services | • Alerter<br>• Clip book<br>• FTP Publishing<br>• HS Admin Service<br>• Messenger<br>• NetMeeting Remote Desktop Sharing<br>• Routing and Remote Access<br>• Simple Mail Transfer Protocol (SMTP)<br>• Simple Network Management Protocol (SNMP) Service<br>• SNMP Trap<br>• Telnet |

| | |
|---|---|
| | • World Wide Web Publishing Services<br>• Computer Browser<br>• Remote Registry<br>• Task Scheduler<br>• Terminal Services<br>• Fax Service<br>• Indexing Service<br>• Remote Desktop Help Session Manager<br>• Universal Plug & Play Device Host<br>• Net logon |
| 6.0 File Permissions | • Harden security permissions for critical files |
| 7.0 Registry Permissions | • Harden security permissions for critical registry keys |
| 8.0 Registry Values<br>8.1 Debugging<br>8.2 Automatic Functions<br>8.3 Networking | • Disable the Dr. Watson debugger and memory dump file<br>• Disable automatically running CD-ROMs<br>• Disable automatic administrator logon<br>• Disable automatic reboot<br>• Strengthen miscellaneous networking settings<br>• Harden the Microsoft TCP/IP stack settings |
| 9.0 Custom PCI Policies<br>9.1 Automatic Logoff<br>9.2 Customer File Protection<br>9.3 USB Removable Device | • Meets PCI Technical Safeguard 314.4(b)(3)<br>• Meets PCI Technical Safeguard 314.4(b)(3)<br>• Meets PCI Physical Safeguards 314.4(c) |

# Appendix C

## New Boundary Technologies PCI Server Template Settings

This chart describes the **Server** security policies contained in Policy Commander that can be used to secure your servers to meet PCI requirements.

For further information, refer to the companion guide, *Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP*, which is available at: *http://www.microsoft.com/technet/security/topics/serversecurity/tcg/tcgch00.mspx*

| Server Role | Policy Commander Policies |
|---|---|
| 1.0 Domain Controller | • Windows Server 2003: High Security - Domain Controller<br>• Windows Server 2003: Enterprise Client - Domain Controller<br>• Windows Server 2003: Legacy Client - Domain Controller<br>• Windows 2000 Server: Domain Controller |
| 2.0 File Server | • Windows Server 2003: High Security - File Server<br>• Windows Server 2003: Enterprise Client - File Server<br>• Windows Server 2003: Legacy Client - File Server<br>• Windows 2000 Server: File Server |
| 3.0 IIS Server | • Windows Server 2003: High Security - IIS Server<br>• Windows Server 2003: Enterprise Client - IIS Server<br>• Windows Server 2003: Legacy Client - IIS Server<br>• Windows 2000 Server: IIS Server |
| 4.0 Infrastructure Server | • Windows Server 2003: High Security - Infrastructure Server<br>• Windows Server 2003: Enterprise Client - Infrastructure Server<br>• Windows Server 2003: Legacy Client - Infrastructure Server<br>• Windows 2000 Server: Infrastructure Server |
| 5.0 Member Servers | • Windows Server 2003: High Security – Member Server<br>• Windows Server 2003: Enterprise Client - Member Server<br>• Windows Server 2003: Legacy Client - Member Server<br>• Windows 2000 Server: Member Server |
| 6.0 Print Servers | • Windows Server 2003: High Security – Print Server<br>• Windows Server 2003: Enterprise Client - Print Server<br>• Windows Server 2003: Legacy Client - Print Server<br>• Windows 2000 Server: Print Server |
| 6.0 Certificate Services Server | • Windows Server 2003: Enterprise Client - Cert Services Server |
| 7.0 IAS Server | • Windows Server 2003: Enterprise Client - IAS Server |