



Mirrored Storage, Inc.

Payment Card Information - PCI

White Paper presented by:

Mirrored Storage, Inc.

ONLINE BACKUP SOFTWARE

<http://MirroredStorage.com>

Introduction

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Build and Maintain a Secure Network

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

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

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

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Specific Requirements

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.	No wireless access is available on the appliance directly. Only wired access is available but if a wireless router is available the appliance can reach machines that are using it.
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.	All unnecessary components are stripped from the appliance and utilized industry leading anti-virus systems with at least daily automatic updates applied.
2.2.1 Implement only one primary function per server.	The appliance is only used to run the remote backup software that encrypts the data and streams it to the Mirrored Storage primary data center.
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	The Appliance contains none of these functions.
2.3 Encrypt all non-console administrative access.	A variety of encryptions methods are use for the streaming of data to the Mirrored Storage data center.
2.4 Shared hosting providers must protect each	All information is encrypted and stored in

entity's hosted environment and data.	different files structures from each other.
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	You can work with the administrator to determine the retention period of data at the Mirrored Storage data center(s) and the number of version stored. We do NOT automatically delete files.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements, 3.2.1 through 3.2.3:	Not key information is ever generated, stored or know at the Mirrored Storage data center. Only the Appliance has the information when installed and they not kept there either.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	The key is not associated with the Appliance nor stored there.
3.6.1 Generation of strong cryptographic keys	The values of the encryption key include several components including the value determined at installation. All components are required to access the correct decrypted information.
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	The Appliance utilizes industry leading anti-virus systems with at least daily automatic updates applied.
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Mirrored Storage is compliant with this requirement.
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	Mirrored Storage is compliant with this requirement.
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	The Appliance is setup to keep the Operating Systems, anti-virus and our software is updated for you when an update is available.
6.3.1 Testing of all security patches, and system and software configuration changes before deployment	We do all the testing for you before we deploy any changes.
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities 7.1.2 Assignment of privileges is based on individual personnel's job classification and function 7.1.3 Requirement for an authorization form signed by management that specifies required privileges 7.1.4 Implementation of an automated access control system	The Mirrored Storage data centers are compliant with all of these requirements.
8.1 Assign all users a unique ID before allowing them to access system components or cardholder	The Mirrored Storage data centers are compliant with all of these requires.

data.	
<p>8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Password or passphrase <input type="checkbox"/> Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys) 	Mirrored Storage is compliant with this requirement.
<p>9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.</p> <p>9.1.2 Restrict physical access to publicly accessible network jacks</p> <p>9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.</p>	Mirrored Storage is compliant with all of these requirements.
<p>9.5 Store media backups in a secure location, preferably in an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.</p>	Mirrored Storage is compliant with this requirement.
<p>9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.</p>	Mirrored Storage is compliant with this requirement.
<p>9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.</p>	Mirrored Storage logs all backups and restores in great detail.
<p>10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.</p>	Mirrored Storage is compliant with this requirement.
<p>10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).</p>	Mirrored Storage is compliant with this requirement.
<p>A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.</p>	Mirrored Storage is compliant with this requirement.
<p>A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.</p>	Mirrored Storage is compliant with this requirement.
<p>A.1.2 Restrict each entity's access and privileges to own cardholder data environment only.</p>	Mirrored Storage is compliant with this requirement.
<p>A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.</p>	Mirrored Storage is compliant with this requirement.
<p>A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.</p>	Mirrored Storage is compliant with this requirement.

Summary

There are several aspects of PCI DSS compliance that [Mirrored Storage](#) can satisfy listed in detail above. First and most importantly our security methods are fully compliant with PCI requirements and since the key is only available to the customer your data stored in our data centers is completely secure.

Acknowledgements and Sources:

PCI Security Standards Council; *Navigating PCI DSS: Understanding the Intent of the Requirements, v1.2*

Media Contact information:
John Neibel, President & Founder
[Mirrored Storage, Inc.](#)
P. 214-550-0550



Copyright © 2010, [Mirrored Storage, Inc.](#) Any reuse without the expressed written permission of [Mirrored Storage, Inc.](#) is prohibited.