



# Windows Azure™

## Customer PCI Guide

January 2014

Version 1.0

**Prepared by:**

Neohapsis, Inc.  
217 North Jefferson St., Suite 200  
Chicago, IL 60661

New York | Chicago | Dallas | Seattle

This document contains and constitutes information that is proprietary to Neohapsis, Inc. (“Neohapsis”). Redistribution of this document in part or in full is restricted without prior written permission.

The contents of this document do not constitute legal advice provided by Neohapsis or Microsoft. Neohapsis’ offer of services or deliverables that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such.

All copyrights and trademarks contained herein are the property of their respective owners.

# Table of Contents

<b>AZURE CUSTOMER PCI GUIDE OVERVIEW .....</b>	<b>4</b>
<b>Requirement 1: Install and maintain a firewall configuration to protect cardholder data ..</b>	<b>5</b>
<b>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters .....</b>	<b>6</b>
<b>Requirement 3: Protect stored cardholder data.....</b>	<b>7</b>
<b>Requirement 4: Encrypt transmission of cardholder data across open, public networks ....</b>	<b>9</b>
<b>Requirement 5: Use and regularly update anti-virus software or programs.....</b>	<b>9</b>
<b>Requirement 6: Develop and maintain secure systems and applications .....</b>	<b>10</b>
<b>Requirement 7: Restrict access to cardholder data by business need to know .....</b>	<b>11</b>
<b>Requirement 8: Assign a unique ID to each person with computer access. ....</b>	<b>12</b>
<b>Requirement 9: Restrict physical access to cardholder data. ....</b>	<b>13</b>
<b>Requirement 10: Track and monitor all access to network resources and cardholder data. ....</b>	<b>15</b>
<b>Requirement 11: Regularly test security systems and processes. ....</b>	<b>17</b>
<b>Requirement 12: Maintain a policy that addresses information security for all personnel</b>	<b>18</b>

## Azure Customer PCI Guide Overview

Neohapsis, Inc. performed a Payment Card Industry Data Security Standard (PCI DSS) assessment for Windows Azure, based on PCI DSS 2.0.

The table below contains all of the PCI DSS requirements and related testing procedures. The responsibility for each control has been categorized as one of the following; 1.) Windows Azure, 2.) Joint or 3.) Customer. The organization(s) identified in the Responsibility column is responsible for ensuring that they achieve PCI DSS compliance for that requirement.

Using this information, Azure Customers can clearly communicate requirements to their own PCI Qualified Security Assessors (QSAs), thereby eliminating duplicative testing and reducing the efforts of their own PCI certification.

The requirements that identify “**Windows Azure**” as having responsibility have been assessed by Neohapsis and Windows Azure has been found to be fully PCI DSS compliant for those requirements as of December 31, 2013. Windows Azure “Customer” bears no responsibility to meet PCI DSS compliance for these requirements.

For the requirements identified as “**Joint**” responsibility, Neohapsis has determined that Windows Azure is fully PCI DSS compliant for these requirements as of December 31, 2013; however, action must still be taken by the Windows Azure Customers to achieve PCI DSS compliance for these requirements.

For the requirements identified as “**Customer**” responsibility, these requirements were NOT tested as part of this PCI DSS assessment by Neohapsis for Windows Azure. It is the sole responsibility of each Windows Azure customer to achieve PCI DSS compliance for these requirements.




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










Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted 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 untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.








Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Requirement	Responsibility
<b>1.1</b> Establish firewall and router configuration standards that include the following:	
<b>1.1.1</b> A formal process for approving and testing all network connections and changes to the firewall and router configurations.	
<b>1.1.2</b> Current network diagram with all connections to cardholder data, including any wireless networks.	<b>Joint</b>
<b>1.1.3</b> Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	
<b>1.1.4</b> Description of groups, roles, and responsibilities for logical management of network components.	
<b>1.1.5</b> Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	<b>Joint</b>
<b>1.1.6</b> Requirement to review firewall and router rule sets at least every six months.	<b>Joint</b>

PCI DSS Requirement	Responsibility
<b>1.2</b> Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	
<b>1.2.1</b> Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	<b>Joint</b>
<b>1.2.2</b> Secure and synchronize router configuration files.	 Windows Azure
<b>1.2.3</b> Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	 Windows Azure
<b>1.3</b> Prohibit direct public access between the Internet and any system component in the cardholder data environment.	
<b>1.3.1</b> Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	 Windows Azure
<b>1.3.2</b> Limit inbound Internet traffic to IP addresses within the DMZ.	 Windows Azure
<b>1.3.3</b> Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	 Windows Azure
<b>1.3.4</b> Do not allow internal addresses to pass from the Internet into the DMZ.	 Windows Azure
<b>1.3.5</b> Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	<b>Joint</b>
<b>1.3.6</b> Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	 Windows Azure
<b>1.3.7</b> Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	 Windows Azure
<b>1.3.8</b> Do not disclose private IP addresses and routing information to unauthorized parties.	 Windows Azure
<b>1.4</b> Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	<b>Customer</b>

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


Malicious individuals (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 by hacker communities and are easily determined via public information.

PCI DSS Requirements	Responsibility
<b>2.1</b> Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	 Windows Azure
<b>2.1.1</b> 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.	<b>Customer</b>
<b>2.2</b> 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.	 Windows Azure
<b>2.2.1</b> Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	<b>Joint</b>
<b>2.2.2</b> Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system.	 Windows Azure
<b>2.2.3</b> Configure system security parameters to prevent misuse.	 Windows Azure
<b>2.2.4</b> Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	 Windows Azure
<b>2.3</b> Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	 Windows Azure
<b>2.4</b> Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in <i>Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</i> .	 Windows Azure

### Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other 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 unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of “strong cryptography” and other PCI DSS terms.

PCI DSS Requirements	Responsibility
<b>3.1</b> Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes, as follows:	
<b>3.1.1</b> Implement a data retention and disposal policy.	<b>Customer</b>
<b>3.2</b> Do not store sensitive authentication data after authorization (even if encrypted).	<b>Customer</b>
<b>3.2.1</b> Do not store the full contents of any track.	<b>Customer</b>
<b>3.2.2</b> Do not store the card-verification code or value.	<b>Customer</b>
<b>3.2.3</b> Do not store the personal identification number (PIN) or the encrypted PIN block.	<b>Customer</b>
<b>3.3</b> Mask PAN when displayed.	<b>Customer</b>
<b>3.4</b> Render PAN unreadable anywhere it is stored.	<b>Customer</b>
<b>3.4.1</b> 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.	
<b>3.5</b> Protect any keys used to secure cardholder data against disclosure and misuse:	
<b>3.5.1</b> Restrict access to cryptographic keys to the fewest number of custodians necessary.	<b>Customer</b>
<b>3.5.2</b> Store cryptographic keys securely in the fewest possible locations and forms.	<b>Customer</b>
<b>3.6</b> Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	<b>Customer</b>
<b>3.6.1</b> Generation of strong cryptographic keys.	<b>Customer</b>
<b>3.6.2</b> Secure cryptographic key distribution.	<b>Customer</b>
<b>3.6.3</b> Secure cryptographic key storage.	<b>Customer</b>
<b>3.6.4</b> Cryptographic key changes for keys that have reached the end of their cryptoperiod.	<b>Customer</b>
<b>3.6.5</b> Retirement or replacement of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.	<b>Customer</b>
<b>3.6.6</b> If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control	<b>Customer</b>



PCI DSS Requirements	Responsibility
<b>3.6.7</b> Prevention of unauthorized substitution of cryptographic keys.	<b>Customer</b>
<b>3.6.8</b> Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	<b>Customer</b>




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

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Requirements	Responsibility
<b>4.1</b> Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	<b>Joint</b>
<b>4.1.1</b> Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	<b>Customer</b>
<b>4.2</b> Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	<b>Customer</b>

## Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business approved activities including employees’ e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS Requirements	Responsibility
<b>5.1</b> Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	 <b>Windows Azure</b>
<b>5.1.1</b> Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	 <b>Windows Azure</b>
<b>5.2</b> Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	 <b>Windows Azure</b>

## Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

PCI DSS Requirements	Responsibility
<b>6.1</b> Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	<b>Joint</b>
<b>6.2</b> Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	<b>Joint</b>
<b>6.3</b> Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS, and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	<b>Customer</b>
<b>6.3.1</b> Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers.	<b>Customer</b>
<b>6.3.2</b> Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	<b>Customer</b>
<b>6.4</b> Follow change control processes and procedures for all changes to system components. The processes must include the following:	
<b>6.4.1</b> Separate development/test and production environments.	<b>Customer</b>
<b>6.4.2</b> Separation of duties between development/test and production environments.	<b>Customer</b>
<b>6.4.3</b> Production data (live PANs) are not used for testing or development.	<b>Customer</b>
<b>6.4.4</b> Removal of test data and accounts before production systems become active.	<b>Customer</b>
<b>6.4.5</b> Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	
<b>6.4.5.1</b> Documentation of impact.	<b>Joint</b>
<b>6.4.5.2</b> Documented change approval by authorized parties.	<b>Joint</b>
<b>6.4.5.3</b> Functionality testing to verify that the change does not adversely impact the security of the system.	<b>Joint</b>
<b>6.4.5.4</b> Back-out procedures.	<b>Joint</b>

PCI DSS Requirements	Responsibility
<b>6.5</b> Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following:	
<b>6.5.1</b> Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	<b>Customer</b>
<b>6.5.2</b> Buffer overflow.	<b>Customer</b>
<b>6.5.3</b> Insecure cryptographic storage.	<b>Customer</b>
<b>6.5.4</b> Insecure communications.	<b>Customer</b>
<b>6.5.5</b> Improper error handling.	<b>Customer</b>
<b>6.5.6</b> All “High” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).	<b>Customer</b>
<b>6.5.7</b> Cross-site scripting (XSS).	<b>Customer</b>
<b>6.5.8</b> Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal).	<b>Customer</b>
<b>6.5.9</b> Cross-site request forgery (CSRF).	<b>Customer</b>
<b>6.6</b> For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: <ul style="list-style-type: none"> <li>Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes</li> <li>Installing a web-application firewall in front of public-facing web applications</li> </ul>	<b>Customer</b>

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

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.




“Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.



PCI DSS Requirements	Responsibility
<b>7.1</b> Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	
<b>7.1.1</b> Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.	<b>Joint</b>

PCI DSS Requirements	Responsibility
<b>7.1.2</b> Assignment of privileges is based on individual personnel's job classification and function.	<b>Joint</b>
<b>7.1.3</b> Requirement for a documented approval by authorized parties specifying required privileges.	<b>Joint</b>
<b>7.1.4</b> Implementation of an automated access control system.	<b>Joint</b>
<b>7.2</b> Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	
<b>7.2.1</b> Coverage of all system components.	<b>Joint</b>
<b>7.2.2</b> Assignment of privileges to individuals based on job classification and function.	<b>Joint</b>
<b>7.2.3</b> Default "deny-all" setting.	<b>Joint</b>

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

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.










PCI DSS Requirements	Responsibility
<b>8.1</b> Assign all users a unique ID before allowing them to access system components or cardholder data.	<b>Joint</b>
<b>8.2</b> In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: <ul style="list-style-type: none"> <li>• Something you know, such as a password or passphrase</li> <li>• Something you have, such as a token device or smart card</li> <li>• Something you are, such as a biometric</li> </ul>	
<b>8.3</b> Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.	
<b>8.4</b> Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	<b>Joint</b>
<b>8.5</b> Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	
<b>8.5.1</b> Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	<b>Joint</b>
<b>8.5.2</b> Verify user identity before performing password resets.	

PCI DSS Requirements	Responsibility
<b>8.5.3</b> Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	<b>Joint</b>
<b>8.5.4</b> Immediately revoke access for any terminated users.	<b>Joint</b>
<b>8.5.5</b> Remove/disable inactive user accounts at least every 90 days.	 Windows Azure
<b>8.5.6</b> Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	 Windows Azure
<b>8.5.7</b> Communicate authentication procedures and policies to all users who have access to cardholder data.	<b>Joint</b>
<b>8.5.8</b> Do not use group, shared, or generic accounts and passwords, or other authentication methods.	<b>Joint</b>
<b>8.5.9</b> Change user passwords at least every 90 days.	<b>Joint</b>
<b>8.5.10</b> Require a minimum password length of at least seven characters.	<b>Joint</b>
<b>8.5.11</b> Use passwords containing both numeric and alphabetic characters.	<b>Joint</b>
<b>8.5.12</b> 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.	<b>Joint</b>
<b>8.5.13</b> Limit repeated access attempts by locking out the user ID after not more than six attempts.	<b>Joint</b>
<b>8.5.14</b> Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	<b>Joint</b>
<b>8.5.15</b> If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	<b>Joint</b>
<b>8.5.16</b> Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	<b>Joint</b>

## Requirement 9: Restrict physical access to cardholder data.

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. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.















PCI DSS Requirements	Responsibility
<b>9.1</b> Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	 Windows Azure
<b>9.1.1</b> Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	 Windows Azure
<b>9.1.2</b> Restrict physical access to publicly accessible network jacks.	 Windows Azure
<b>9.1.3</b> Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	 Windows Azure
<b>9.2</b> Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	 Windows Azure
<b>9.3</b> Make sure all visitors are handled as follows:	
<b>9.3.1</b> Authorized before entering areas where cardholder data is processed or maintained.	 Windows Azure
<b>9.3.2</b> Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	 Windows Azure
<b>9.3.3</b> Asked to surrender the physical token before leaving the facility or at the date of expiration.	 Windows Azure
<b>9.4</b> Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor’s name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	 Windows Azure
<b>9.5</b> Store media back-ups in a secure location, preferably 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.	<b>Joint</b>
<b>9.6</b> Physically secure all media.	<b>Joint</b>
<b>9.7</b> Maintain strict control over the internal or external distribution of any kind of media, including the following:	<b>Joint</b>
<b>9.7.1</b> Classify media so the sensitivity of the data can be determined.	<b>Joint</b>

PCI DSS Requirements	Responsibility
<b>9.7.2</b> Send the media by secured courier or other delivery method that can be accurately tracked.	<b>Joint</b>
<b>9.8</b> Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	<b>Joint</b>
<b>9.9</b> Maintain strict control over the storage and accessibility of media.	<b>Joint</b>
<b>9.9.1</b> Properly maintain inventory logs of all media and conduct media inventories at least annually.	<b>Joint</b>
<b>9.10</b> Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:	<b>Customer</b>
<b>9.10.1</b> Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	<b>Customer</b>
<b>9.10.2</b> Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	<b>Customer</b>



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

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS Requirements	Responsibility
<b>10.1</b> Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	 <b>Windows Azure</b>
<b>10.2</b> Implement automated audit trails for all system components to reconstruct the following events:	
<b>10.2.1</b> All individual accesses to cardholder data.	<b>Customer</b>
<b>10.2.2</b> All actions taken by any individual with root or administrative privileges.	 <b>Windows Azure</b>
<b>10.2.3</b> Access to all audit trails.	 <b>Windows Azure</b>
<b>10.2.4</b> Invalid logical access attempts.	 <b>Windows Azure</b>
<b>10.2.5</b> Use of identification and authentication mechanisms.	 <b>Windows Azure</b>
<b>10.2.6</b> Initialization of the audit logs.	 <b>Windows Azure</b>






PCI DSS Requirements	Responsibility
<b>10.2.7</b> Creation and deletion of system-level objects.	 Windows Azure
<b>10.3</b> Record at least the following audit trail entries for all system components for each event:	
<b>10.3.1</b> User identification.	 Windows Azure
<b>10.3.2</b> Type of event.	 Windows Azure
<b>10.3.3</b> Date and time.	 Windows Azure
<b>10.3.4</b> Success or failure indication.	 Windows Azure
<b>10.3.5</b> Origination of event.	 Windows Azure
<b>10.3.6</b> Identity or name of affected data, system component, or resource.	 Windows Azure
<b>10.4</b> Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	
<b>10.4.1</b> Critical systems have the correct and consistent time.	 Windows Azure
<b>10.4.2</b> Time data is protected.	 Windows Azure
<b>10.4.3</b> Time settings are received from industry-accepted time sources.	 Windows Azure
<b>10.5</b> Secure audit trails so they cannot be altered.	
<b>10.5.1</b> Limit viewing of audit trails to those with a job-related need.	<b>Joint</b>
<b>10.5.2</b> Protect audit trail files from unauthorized modifications.	 Windows Azure
<b>10.5.3</b> Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	 Windows Azure
<b>10.5.4</b> Write logs for external-facing technologies onto a log server on the internal LAN.	 Windows Azure
<b>10.5.5</b> Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.	 Windows Azure



PCI DSS Requirements	Responsibility
<b>10.6</b> Review logs for all system components at least daily.	 Windows Azure
<b>10.7</b> Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.	 Windows Azure


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

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Requirements	Responsibility
<b>11.1</b> Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.	 Windows Azure
<b>11.2</b> 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).	 Windows Azure
<b>11.2.1</b> Perform quarterly internal vulnerability scans.	<b>Joint</b>
<b>11.2.2</b> Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).	<b>Customer</b>
<b>11.2.3</b> Perform internal and external scans after any significant change.	 Windows Azure
<b>11.3</b> Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification. These penetration tests must include the following:	<b>Customer</b>
<b>11.3.1</b> Network-layer penetration tests.	<b>Customer</b>
<b>11.3.2</b> Application-layer penetration tests.	<b>Customer</b>
<b>11.4</b> Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	 Windows Azure
<b>11.5</b> Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	 Windows Azure

## Requirement 12: Maintain a policy that addresses information security for all personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.

PCI DSS Requirements	Responsibility
<b>12.1</b> Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	<b>Joint</b>
<b>12.1.1</b> Addresses all PCI DSS requirements.	<b>Joint</b>
<b>12.1.2</b> Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	<b>Joint</b>
<b>12.1.3</b> Includes a review at least annually and updates when the environment changes.	<b>Joint</b>
<b>12.2</b> Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	<b>Joint</b>
<b>12.3</b> Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:	
<b>12.3.1</b> Explicit approval by authorized parties	<b>Joint</b>
<b>12.3.2</b> Authentication for use of the technology.	<b>Joint</b>
<b>12.3.3</b> A list of all such devices and personnel with access.	<b>Joint</b>
<b>12.3.4</b> Labeling of devices to determine owner, contact information and purpose.	<b>Joint</b>
<b>12.3.5</b> Acceptable uses of the technology.	<b>Joint</b>
<b>12.3.6</b> Acceptable network locations for the technologies.	<b>Joint</b>
<b>12.3.7</b> List of company-approved products.	<b>Joint</b>
<b>12.3.8</b> Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.	
<b>12.3.9</b> Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	<b>Joint</b>

PCI DSS Requirements	Responsibility
<b>12.3.10</b> For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	<b>Joint</b>
<b>12.4</b> Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	<b>Joint</b>
<b>12.5</b> Assign to an individual or team the following information security management responsibilities:	
<b>12.5.1</b> Establish, document, and distribute security policies and procedures.	<b>Joint</b>
<b>12.5.2</b> Monitor and analyze security alerts and information, and distribute to appropriate personnel.	<b>Joint</b>
<b>12.5.3</b> Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	<b>Joint</b>
<b>12.5.4</b> Administer user accounts, including additions, deletions, and modifications	<b>Joint</b>
<b>12.5.5</b> Monitor and control all access to data.	<b>Joint</b>
<b>12.6</b> Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	<b>Joint</b>
<b>12.6.1</b> Educate personnel upon hire and at least annually.	<b>Joint</b>
<b>12.6.2</b> Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	<b>Joint</b>
<b>12.7</b> Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	<b>Joint</b>
<b>12.8</b> If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	
<b>12.8.1</b> Maintain a list of service providers.	<b>Customer</b>
<b>12.8.2</b> Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	<b>Customer</b>
<b>12.8.3</b> Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	<b>Customer</b>
<b>12.8.4</b> Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	<b>Customer</b>
<b>12.9</b> Implement an incident response plan. Be prepared to respond immediately to a system breach.	

PCI DSS Requirements	Responsibility
<b>12.9.1</b> Create the incident response plan to be implemented in the event of system breach.	<b>Joint</b>
<b>12.9.2</b> Test the plan at least annually.	<b>Joint</b>
<b>12.9.3</b> Designate specific personnel to be available on a 24/7 basis to respond to alerts.	<b>Joint</b>
<b>12.9.4</b> Provide appropriate training to staff with security breach response responsibilities.	<b>Joint</b>
<b>12.9.5</b> Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.	<b>Joint</b>
<b>12.9.6</b> Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	<b>Joint</b>