Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire D

and Attestation of Compliance

for

Tucows

PCI Questionnaire 2011

All other Merchants

Version : 1.2

Part 2. Merchant Organization Information

Company Name:	Tucows	DBA(s):			
Contact Name:	Garrick Lau	Title:	Director, IT Security and Compliance		
Telephone:	416 538 5442	E-mail:	glau@tucows.com		
Business Address:	96 Mowat Ave,	City:	Toronto		
State/Province:	Ontario	Country:	Canada	ZIP:	M5M1Y5
URL:	www.tucowsinc.com				

Part 2a. Business Information

Brief Description:	Tucows provides domain names, E-mail and other internet services through our extensive reseller network, called our OpenSRS group. We sell these services directly to consumers and small businesses through our unified Retail group known as Hover.
Transactions per year:	350,000
Locations:	96 Mowat Avenue, Toronto, Ontario M5M 1Y5

Part 2b. Relationships

Processor:	Litle & Co	Gateway:	
Web-Hosting:		Shopping Cart:	
Co-Locations:	Q9 Networks, Equinix Inc	Others:	

Part 2c. Transaction Processing - Point of Sale software/hardware details

Part 3. PCI DSS Validation

Based on the results noted in the SAQ D dated November 29, 2011, Tucows asserts the following compliance status:

Compliant	All the sections of the PCI SAQ are complete, and all questions answered "yes", resulting in an overall COMPLIANT rating, thereby Tucows has demonstrated full compliance with the PCI DSS.

Part 3a. Confirmation of Compliant Status

Merchant/Service Provider confirms:

- PCI DSS Self-Assessment Questionnaire D, Version 1.2, was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (i.e. track) data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage subsequent to transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. Merchant Acknowledgement

Signature:	*Electronically Signed*	Date:	November 29, 2011
Name:	Mike Cooperman	Title:	Chief Financial Officer
Company Name:	Tucows Incorporated		

Submitted 11/29/2011

Part 4. Rating the Assessment and Action Plan for Compliance

Compliance of the Self-Assessment Questionnaire is rated as follows:

In each section IF...	THEN the section rating is...
ALL questions are answered with "Yes", "N/A" or "Compensating Controls"	✅ - The merchant or service provider is compliant with the self-assessment portion of the PCI Data Security Standard. Note: If "N/A" or "Compensating Controls" is marked, attach a brief explanation.
ANY questions are unanswered or answered with "No"	⛔ - The merchant or service provider is not considered compliant. To reach compliance, the risk(s) must be resolved and the self-assessment must be retaken to demonstrate compliance.

No.	PCI DSS Requirement	Rating	Remediation Plan or Comments	Remediation Target Date
1	Install and maintain a firewall configuration to protect data	✅		
2	Do not use vendor-supplied defaults for system passwords and other security parameters	✅		
3	Protect stored cardholder data	✅		
4	Encrypt transmission of cardholder data and sensitive information across public networks	✅		
5	Use and regularly update anti-virus software	✅		
6	Develop and maintain secure system and applications	✅		
7	Restrict access to data by business need-to-know	✅		
8	Assign a unique ID to each person with computer access	✅		
9	Restrict physical access to cardholder data	✅		
10	Track and monitor all access to network resources and cardholder data	✅		
11	Regularly test security systems and processes	✅		
12	Maintain a policy that addresses information security for employees and contractors	✅		

Build and Maintain a Secure Network

Requirement 1 : Install and maintain a firewall configuration to protect data				
1.1	Do established firewall configuration standards include the following?			
1.1.1	A formal process for approving and testing all external network connections and changes to the firewall and router configurations?		Yes	✓
1.1.2	Current network diagrams with all connections to cardholder data, including any wireless networks?		Yes	✓
1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?		Yes	✓
1.1.4	Description of groups, roles, and responsibilities for logical management of network components?		Yes	✓
1.1.5	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?		Yes	✓
1.1.6	Requirement to review firewall and router rule sets at least every six months?		Yes	✓
1.2	Does the firewall configuration restrict connections between untrusted networks and any system in the cardholder data environment as follows: Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.			
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment?		Yes	✓
1.2.2	Secure and synchronize router configuration files?		Yes	✓
1.2.3	Include installation of 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.? *Comment:* *No wiresless networks exist in the cardholder environment and the Tucows wireless environments are considered "untrusted" and treated as "public / internet" type networks protected by firewalls and requiring VPN to access any internal Tucows infrastructure.*		Yes	✓
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment?			
1.3.1	Is a DMZ implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder environment?		Yes	✓
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?		Yes	✓
1.3.3	Are direct routes prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?		Yes	✓
1.3.4	Are internal addresses prohibited from passing from the Internet into the DMZ?		Yes	✓
1.3.5	Is outbound traffic restricted from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ?		Yes	✓
1.3.6	Is stateful inspection, also known as dynamic packet filtering, implemented (that is, only established connections are allowed into the network)?		Yes	✓
1.3.7	Is the database placed in an internal network zone, segregated from the DMZ?		Yes	✓
1.3.8	Has IP-masquerading been implemented to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space? Use Network address translation (NAT) technologies - for example, port address translation (PAT). ?		Yes	✓
1.4	Has personal firewall software been installed 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?		Yes	✓
Requirement 2 : Do not use vendor-supplied defaults for system passwords and other security parameters				
2.1	Are vendor-supplied defaults always changed before installing a system on the network? Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.		Yes	✓
2.1.1	(a)	Are defaults** for wireless environments connected to the cardholder data environment or transmitting cardholder data changed before installing a wireless system? ** Such wireless environment defaults include but are not limited to default wireless encryption keys, passwords, and SNMP community strings. *Comment:* *There are no wireless networking environments directly connected to the Tucows data environment.*	N/A	✓

	2.1.1	(b)	Are wireless device security settings enabled for strong encryption technology for authentication and transmissions?	Yes	✓
2.2		(a)	Have configuration standards been developed for all system components?	Yes	✓
2.2		(b)	Do these standards address all known security vulnerabilities and are they consistent with industry-accepted system hardening standards - for example, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS)? *Comment:* *New system implementations undergo a PCI scan as well as internal scans during QA and pre-production and immediately following production implementation.*	Yes	✓
2.2		(c)	Do controls ensure the following:		
	2.2.1		Is only one primary function implemented per server?	Yes	✓
	2.2.2		Are all unnecessary and insecure services and protocols disabled (services and protocols not directly needed to perform the devices' specified function)?	Yes	✓
	2.2.3		Are system security parameters configured to prevent misuse?	Yes	✓
	2.2.4		Has all unnecessary functionality - such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers - been removed?	Yes	✓
2.3			Is all non-console administrative access encrypted? Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	Yes	✓
2.4			If you are a shared hosting provider, are your systems configured to protect each entity's hosted environment and cardholder data? See Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for specific requirements that must be met. *Comment:* *We are not a shared hosting provider and do not host or share the cardholder environment.*	N/A	✓

Protect Cardholder Data

Requirement 3 : Protect stored cardholder data				
3.1	(a)	Is storage of cardholder data kept to a minimum, and is storage amount and retention time limited to that which is required for business, legal, and/or regulatory purposes?	Yes	✓
3.1	(b)	Is there a data-retention and disposal policy, and does it include limitations as stated in (a) above?	Yes	✓
3.2		Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)? *Comment:* *The storage of sensitive authentication data is only performed on volitile memory only for the purposes of transmitting the data to our processor and is immediately removed. No sensitive authentication data is ever stored on non-volitile memory.*	Yes	✓
3.2.1		Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: · The cardholder's name, · Primary account number (PAN), · Expiration date, and · Service code To minimize risk, store only these data elements as needed for business. NEVER store the card verification code or value or PIN verification value data elements. Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.	Yes	✓
3.2.2		Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.	Yes	✓
3.2.3		Do not store the personal identification number (PIN) or the encrypted PIN block.	Yes	✓
3.3		Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed). Note: · This requirement does not apply to employees and other parties with a specific need to see the full PAN; This requirement does not supersede stricter requirements in place for displays of cardholder data - for example, for point-of-sale (POS) receipts.	Yes	✓
3.4		Is PAN, at a minimum, rendered 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? · One-way hashes based on strong cryptography Truncation Index tokens and pads (pads must be securely stored) Strong cryptography with associated key management processes and procedures. The MINIMUM account information that must be rendered unreadable is the PAN.If for some reason, a company is unable to render the PAN unreadable, refer to Appendix B: "Compensating Controls."Note: "Strong cryptography" is defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms. *Comment:* *Tucows uses strong encryption using 4096 bit PGP keys. At this time, the sole key custodian is our CEO. We will soon add our CFO. The key was created by the Director of IT Security and witnessed by a Security Specialist, written to CDROM and given directly to the CEO who keeps it under lock and key in his office.*	Yes	✓
3.4.1		If disk encryption (rather than file-or column-level database encryption) is used:		
3.4.1	(a)	Is logical access managed independently of native operating system access control mechanisms (for example, by not using local user account databases)? *Comment:* *Disk encryption is not used.*	N/A	✓
3.4.1	(b)	Are decryption keys independent of user accounts? *Comment:* *Disk encryption is not used.*	N/A	✓
3.5		Are encryption keys used for encryption of cardholder data protected against both disclosure and misuse? *Comment:* *Tucows uses strong encryption using 4096 bit PGP keys. At this time, the key custodians are our CEO and CFO. The key was created by the Director of IT Security and witnessed by a Security Specialist, written to CDROM and given directly to the CEO and CFO who both keep it under lock and key in thier offices.*	Yes	✓
3.5.1		Is access to keys restricted to the fewest number of custodians necessary?	Yes	✓
3.5.2		Are cryptographic keys stored securely, and in the fewest possible locations and forms?	Yes	✓
3.6	(a)	Are all key-management processes and procedures for keys used for encryption of cardholder data, fully documented and implemented?	Yes	✓
3.6	(b)	Are all key-management processes and procedures for keys used for encryption of cardholder data, fully documented and implemented?		

3.6.1	Generation of strong cryptographic keys	Yes	
3.6.2	Secure cryptographic key distribution	Yes	
3.6.3	Secure cryptographic key storage	Yes	
3.6.4	Periodic changing of keys · As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically · At least annually.	Yes	
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys	Yes	
3.6.6	Split knowledge and establishment of dual control of cryptographic keys	Yes	
3.6.7	Prevention of unauthorized substitution of cryptographic keys	Yes	
3.6.8	Requirement for cryptographic-key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.	Yes	

Requirement 4 : Encrypt transmission of cardholder data and sensitive information across public networks			
4.1	Are strong cryptography and security protocols, such as SSL/TLS or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks? Examples of open, public networks that are in scope of the PCI DSS are the Internet, wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).	Yes	
4.1.1	Are industry best practices (for example, IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment? Notes: · For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. · For current wireless implementations, it is prohibited to use WEP after June 30, 2010. *Comment:* *While we do implement industry best practices using strong encryption for wiresless technologies, there are no Wireless networks connecting directly to the cardholder data environment.*	N/A	
4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)?	Yes	

Maintain a Vulnerability Management Program

Requirement 5 : Use and regularly update anti-virus software			
5.1	Is anti-virus software deployed on all systems, particularly personal computers and servers, commonly affected by malicious software?	Yes	✓
5.1.1	Are all anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software?	Yes	✓
5.2	Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?	Yes	✓
Requirement 6 : Develop and maintain secure system and applications			
6.1 (a)	Do all system components and software have the latest vendor-supplied security patches installed? *Comment:* *We perform monthly vulnerability scanning and issue change requests as vulnerabilities are identified.*	Yes	✓
6.1 (b)	Are critical security patches installed within one month of release? Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.	Yes	✓
6.2 (a)	Is there a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet)?	Yes	✓
6.2 (b)	Are configuration standards updated as required by PCI DSS Requirement 2.2 to address new vulnerability issues?	Yes	✓
6.3 (a)	Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and do they incorporate information security throughout the software development life cycle?.	Yes	✓
6.3 (b)	Are software applications developed based on industry best practices, and do they incorporate information security throughout the software development life cycle.		
6.3.1	Testing of all security patches and system and software configuration changes before deployment, including but not limited to the following:	Yes	✓
6.3.1.1	Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)	Yes	✓
6.3.1.2	Validation of proper error handling	Yes	✓
6.3.1.3	Validation of secure cryptographic storage	Yes	✓
6.3.1.4	Validation of secure communications	Yes	✓
6.3.1.5	Validation of proper role-based access control (RBAC)	Yes	✓
6.3.2	Separate development/test and production environments?	Yes	✓
6.3.3	Separation of duties between development/test and production environments?	Yes	✓
6.3.4	Production data (live PANs) are not used for testing or development? *Comment:* *No live PANs aside from ones that belong to the actual developers and QA testers are used purely for testing purposes. No PANs that do not explicitly belong to the indivudual testing is ever used.*	Yes	✓
6.3.5	Removal of test data and accounts before production systems become active?	Yes	✓
6.3.6	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers?	Yes	✓
6.3.7	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability? Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel. Web applications are also subject to additional controls, if they are public-facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	Yes	✓
6.4 (a)	Are change control procedures followed for all changes to system components?	Yes	✓
6.4 (b)	Do controls ensure the following:		
6.4.1	Documentation of impact?	Yes	✓
6.4.2	Management sign-off by appropriate parties?	Yes	✓

	6.4.3	Testing of operational functionality?	Yes	✓
	6.4.4	Back-out procedures?	Yes	✓
6.5	(a)	Are all web applications (internal and external, and including web administrative access to application) developed based on secure coding guidelines such as the Open Web Application Security Project Guide?	Yes	✓
6.5	(b)	Is prevention of common coding vulnerabilities covered in software development processes, including the following? Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published However, if and when the OWASP guide is updated, the current version must be used for these requirements.		
	6.5.1	Cross-side scripting (XSS)?	Yes	✓
	6.5.2	Injection flaws, particularly SQL injection? Also consider LDAP and Xpath injection flaws as well as other injection flaws.	Yes	✓
	6.5.3	Malicious file execution?	Yes	✓
	6.5.4	Insecure direct object references?	Yes	✓
	6.5.5	Cross-site request forgery (CSRF)?	Yes	✓
	6.5.6	Information leakage and improper error handling?	Yes	✓
	6.5.7	Broken authentication and session management?	Yes	✓
	6.5.8	Insecure cryptographic storage?	Yes	✓
	6.5.9	Insecure communications?	Yes	✓
	6.5.10	Failure to restrict URL access?	Yes	✓
6.6		For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying either of the following methods? · Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or · Installing a web-application layer firewall in front of public facing web applications.	Yes	✓

Implement Strong Access Control Measures

Requirement 7 : Restrict access to data by business need-to-know				
7.1	(a)	Is access to system components and cardholder data limited to only those individuals whose jobs require such access?	Yes	✓
7.1	(b)	Do access limitations include the following:		
	7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities?	Yes	✓
	7.1.2	Assignment of privileges based on individual personnel's job classification and function?	Yes	✓
	7.1.3	Requirement for an authorization form signed by management that specifies required privileges? *Comment:* *Our automated internal ticketing system is used to process access requests. No access is granted without Security review and proper approval and justification provided by Management. While no signature is taken on a form, the automated ticketing mangement system effectively tracks the management approvals and security review.*	Compensating Controls	✓
	7.1.4	Implementation of an automated access control system?	Yes	✓
7.2	(a)	Is an access control system in place for systems with multiple users to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed?	Yes	✓
7.2	(b)	Does this access control system include the following:		
	7.2.1	Coverage of all system components?	Yes	✓
	7.2.2	Assignment of privileges to individuals based on job classification and function?	Yes	✓
	7.2.3	Default "deny-all" setting?	Yes	✓

Requirement 8 : Assign a unique ID to each person with computer access				
8.1		Are all users assigned a unique ID before allowing them to access system components or cardholder data?	Yes	✓
8.2		In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? · Password or passphrase · Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)	Yes	✓
8.3		Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) 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. *Comment:* *When remote access is granted, a specific certificate is used with the client and provided and is role based. In addition, a remote access control system is utilized and all traffic is encrypted with strong encryption.*	Yes	✓
8.4		Are all passwords encrypted during transmission and storage on all system components?	Yes	✓
8.5		Are proper user authentication and password management controls in place for non-consumer users and administrators on all system components, as follows?		
	8.5.1	Are addition, deletion, and modification of user IDs, credentials, and other identifier objects controlled?	Yes	✓
	8.5.2	Is user identity verified before performing password resets?	Yes	✓
	8.5.3	Are first-time passwords set to a unique value for each user and must each user change their password immediately after the first use?	Yes	✓
	8.5.4	Is access for any terminated users immediately revoked?	Yes	✓
	8.5.5	Are inactive user accounts removed or disabled at least every 90 days?	Yes	✓
	8.5.6	Are accounts used by vendors for remote maintenance enabled only during the time period needed?	Yes	✓
	8.5.7	Are password procedures and policies communicated to all users who have access to cardholder data?	Yes	✓
	8.5.8	Are group, shared, or generic accounts and passwords prohibited?	Yes	✓
	8.5.9	Must user passwords be changed at least every 90 days?	Yes	✓
	8.5.10	Is a minimum password length of at least seven characters required? *Comment:* *Our minimum password length is 8*	Yes	✓

	8.5.11		Must passwords contain both numeric and alphabetic characters? *Comment:* *Our passwords require numeric, alphabet and at least one special character. This is fully automated during password assignment and modification.*	Yes
	8.5.12		Must an individual submit a new password that is different from any of the last four passwords he or she has used? *Comment:* *A previous password is never allowed to be used again.*	Yes
	8.5.13		Are repeated access attempts limited by locking out the user ID after no more than six attempts?	Yes
	8.5.14		Is the lockout duration set to thirty minutes or until administrator enables the user ID?	Yes
	8.5.15		If a session has been idle for more than 15 minutes, must the user re-enter the password to re-activate the terminal?	Yes
	8.5.16		Is all access to any database containing cardholder data authenticated? (This includes access by applications, administrators, and all other users.)	Yes

Requirement 9 : Restrict physical access to cardholder data				
9.1			Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	Yes
	9.1.1	(a)	Do video cameras or other access-control mechanisms monitor individual physical access to sensitive areas? Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.	Yes
	9.1.1	(b)	Is data collected from video cameras reviewed and correlated with other entries?	Yes
	9.1.1	(c)	Is data from video cameras stored for at least three months, unless otherwise restricted by law?	Yes
	9.1.2		Is physical access to publicly accessible network jacks restricted?	Yes
	9.1.3		Is physical access to wireless access points, gateways, and handheld devices restricted? *Comment:* *There are no wireless access points directly connected or within the cardholder environment. Handheld devices may exist but no wireless networks exist to allow potential access.*	N/A
9.2			Are procedures in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible?For purposes of this requirement, an "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.	Yes
9.3			Are all visitors handled as follows:	
	9.3.1		Authorized before entering areas where cardholder data is processed or maintained?	Yes
	9.3.2		Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees? *Comment:* *In addition, no visitors are allowed in the cardholder evironment without an employee escort. Visitors are usually prospective customers or auditors who may be allowed into the facility but are never allowed inside our physically protected datacenter cage. i.e. visitors can "see" the card holder environment as they are within the building but remain outside the protective permimeter of the environment.* *Visitor access devices are never allowed through our protective permimeter into the cardholder environment.*	Yes
	9.3.3		Asked to surrender the physical token before leaving the facility or at the date of expiration?	Yes
9.4		(a)	Is a visitor log in use to maintain a physical audit trail of visitor activity?	Yes
9.4		(b)	Are the visitor's name, the firm represented, and the employee authorizing physical access documented on the log?	Yes
9.4		(c)	Is visitor log retained for a minimum of three months, unless otherwise restricted by law?	Yes
9.5		(a)	Are media backups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?	Yes
9.5		(b)	Is this location's security reviewed at least annually?	Yes
9.6			Are all paper and electronic media that contain cardholder data physically secure?	Yes

9.7	(a)	Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?	Yes	✓
9.7	(b)	Do controls over media include the following:		
9.7.1		Is the media classified so it can be identified as confidential?	Yes	✓
9.7.2		Is the media sent by secured courier or other delivery method that can be accurately tracked?	Yes	✓
9.8		Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals)?	Yes	✓
9.9		Is strict control maintained over the storage and accessibility of media that contains cardholder data?	Yes	✓
9.9.1	(a)	Are inventory logs of all media properly maintained?	Yes	✓
9.9.1	(b)	Are media inventories conducted at least annually?	Yes	✓
9.10		Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:	Yes	✓
9.10.1		Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	Yes	✓
9.10.2		Is electronic media with cardholder data rendered unrecoverable so that cardholder data cannot be reconstructed?	Yes	✓

Regularly Monitor and Test Networks

Requirement 10 : Track and monitor all access to network resources and cardholder data			
10.1	Is a process in place to link all access to system components (especially access done with administrative privileges such as root) to each individual user?	Yes	✓
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:		
10.2.1	All individual user accesses to cardholder data?	Yes	✓
10.2.2	All actions taken by any individual with root or administrative privileges?	Yes	✓
10.2.3	Access to all audit trails?	Yes	✓
10.2.4	Invalid logical access attempts?	Yes	✓
10.2.5	Use of identification and authentication mechanisms?	Yes	✓
10.2.6	Initialization of the audit logs?	Yes	✓
10.2.7	Creation and deletion of system-level object?	Yes	✓
10.3	Are the following audit trail entries recorded for all system components for each event:	Yes	✓
10.3.1	User identification?	Yes	✓
10.3.2	Type of event?	Yes	✓
10.3.3	Date and time?	Yes	✓
10.3.4	Success or failure indication?	Yes	✓
10.3.5	Origination of event?	Yes	✓
10.3.6	Identity or name of affected data, system component, or resource?	Yes	✓
10.4	Are all critical system clocks and times synchronized?	Yes	✓
10.5 (a)	Are audit trails secured so they cannot be altered?	Yes	✓
10.5 (b)	Do controls ensure the following?		
10.5.1	Is viewing of audit trails limited to those with a job-related need?	Yes	✓
10.5.2	Are audit trail files protected from unauthorized modifications?	Yes	✓
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	Yes	✓
10.5.4	Are logs for external-facing technologies written onto a log server on the internal LAN?	Yes	✓
10.5.5	Is file-integrity monitoring or change-detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	Yes	✓
10.6	Are logs for all system components reviewed 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). Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.	Yes	✓
10.7	Is audit trail history retained for at least one year, with a minimum of three months' history immediately available for analysis (for examples, online, archived, or restorable from backup)?	Yes	✓

Requirement 11 : Regularly test security systems and processes			
11.1	Is the presence of wireless access points tested for by using a wireless analyzer at least quarterly or by deploying a wireless IDS/IPS to identify all wireless devices in use? *Comment:* *While we do have IDS deployed in our wireless access points, there are no wireless access points directly connected to the Cardholder data environment.*	N/A	✓

11.2		Are internal and external network vulnerability scans run 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)? 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. *Comment:* *External and internal vulnerability scans are performed on a monthly basis*	Yes	✓
11.3	(a)	Is external and internal penetration testing performed 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)?	Yes	✓
11.3	(b)	Do these penetration tests include the following:		
	11.3.1	Network-layer penetration tests?	Yes	✓
	11.3.2	Application-layer penetration tests?	Yes	✓
11.4	(a)	Are intrusion-detection systems and/or intrusion-prevention systems used to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises?	Yes	✓
11.4	(b)	Are all intrusion-detection and prevention engines kept up to date?	Yes	✓
11.5	(a)	Is file-integrity monitoring software deployed to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and *Comment:* *We do not specifically deploy file-integrity monitoring software in the production cardholder data environment due to the fact that the production environments' non-volitile memory (hard disk) is deployed in a "read only" configuration.*	Compensating Controls	✓
11.5	(b)	Is the software configured to perform critical file comparisons at least weekly? Note: 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). *Comment:* *Due to the Read only deployment configuration, our comparisons are not file integrity, rather code comparisons and deployment package comparisons.*	Yes	✓

Maintain an Information Security Policy

Requirement 12 : Maintain a policy that addresses information security for employees and contractors			
12.1	Is a security policy established, published, maintained, and disseminated, and does it accomplish the following:	Yes	✓
12.1.1	Addresses all PCI DSS requirements?	Yes	✓
12.1.2	Includes an annual process to identify threats and vulnerabilities, and which results in a formal risk assessment?	Yes	✓
12.1.3	Includes a review at least once a year and updates when the environment changes?	Yes	✓
12.2	Are daily operational security procedures developed that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures)?	Yes	✓
12.3 (a)	Are usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all employees and contractors?	Yes	✓
12.3 (b)	Do these usage policies require the following?	Yes	✓
12.3.1	Explicit management approval?	Yes	✓
12.3.2	Authentication for use of the technology?	Yes	✓
12.3.3	A list of all such devices and personnel with access?	Yes	✓
12.3.4	Labeling of devices with owner, contact information, and purpose?	Yes	✓
12.3.5	Acceptable uses of the technologies?	Yes	✓
12.3.6	Acceptable network locations for the technologies?	Yes	✓
12.3.7	List of company-approved products?	Yes	✓
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	Yes	✓
12.3.9	Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use?	Yes	✓
12.3.10	When accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copy, move, and storage of cardholder data onto local hard drives and removable electronic media?	Yes	✓
12.4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?	Yes	✓
12.5	Are the following information security management responsibilities assigned to an individual or team:	Yes	✓
12.5.1	Establishing, documenting, and distributing security policies and procedures?	Yes	✓
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?	Yes	✓
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	Yes	✓
12.5.4	Administering user accounts, including additions, deletions, and modifications?	Yes	✓
12.5.5	Monitoring and controlling all access to data?	Yes	✓
12.6	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?	Yes	✓
12.6.1	Are employees educated upon hire and at least annually? *Comment:* *While we educate employees, we also keep this information directed to those employees who potentially come in contact with cardholder data and for all others, we attempt to not draw too much attention to cardholder data.*	Yes	✓
12.6.2	Are employees required to acknowledge in writing that they have read and understood the company's security policy and procedures?	Yes	✓
12.7	Are potential employees screened to minimize the risk of attacks from internal sources? For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. *Comment:* *While we perform the standard screening of employees via interview and HR, we do not perform any background checking.*	N/A	✓

12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, and do the policies and procedures include the following?	Yes	✓
12.8.1	A list of service providers is maintained.	Yes	✓
12.8.2	A written agreement is maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	Yes	✓
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.	Yes	✓
12.8.4	A program is maintained to monitor service providers' PCI DSS compliance status.	Yes	✓
12.9	Has an incident response plan been implemented to include the following in preparation to respond immediately to a system breach?		
12.9.1 (a)	Has an incident response plan been created to be implemented in the event of system compromise?	Yes	✓
12.9.1 (b)	Does the plan address, at a minimum:		
12.9.1.1	Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum	Yes	✓
12.9.1.2	Specific incident response procedures	Yes	✓
12.9.1.3	Business recovery and continuity procedures	Yes	✓
12.9.1.4	Data back-up processes	Yes	✓
12.9.1.5	Analysis of legal requirements for reporting compromises	Yes	✓
12.9.1.6	Coverage and responses of all critical system components	Yes	✓
12.9.1.7	Reference or inclusion of incident response procedures from the payment brands	Yes	✓
12.9.2	Is the plan tested at least annually?	Yes	✓
12.9.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts? *Comment:* *Specific personnel from each of the technical teams are designated to be available 24/7 in addition, we operate a monitoring NOC team that is staffed 24/7/365*	Yes	✓
12.9.4	Is appropriate training provided to staff with security breach response responsibilities?	Yes	✓
12.9.5	Are alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems included?	Yes	✓
12.9.6	Is process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?	Yes	✓