APPENDIX D

Payment Card Industry Data Security Standards (PCI DSS)

BUILD AND MAINTAIN A SECURE NETWORK (see Requirements 1 & 2)			**Responsible Party**
Requirement 1:	**Install and maintain a firewall and router configuration to protect cardholder data**		**CaTS**
	Overview	All systems must be protected from unauthorized access from the Internet, whether entering the system as E-commerce, employees' Internet based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.	
	1.1	Establish firewall and router configuration standards.	
	1.2	Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	
	1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	
	1.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network.	
Requirement 2:	**Do not use vendor-supplied defaults for system passwords and other security parameters.**		**CaTS & Academic/Administrative Depts.**
	Overview	Hackers (external and internal to the organization) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information. This information, combined with hacker tools that show what devices are on your network can make unauthorized entry a simple task- if you have failed to change the defaults.	
	2.1	Always change vendor-supplied defaults **before** installing a system on the network (for example, include passwords, simple network, management protocol (SNMP) community strings, and elimination of unnecessary accounts).	
	2.2	Develop configuration standards for all system components.	**CaTS**
	2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	
	2.4	Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in the PCI DSS Requirements for Shared Hosting Providers.	**CaTS & Academic/Administrative Depts.**
PROTECT CARDHOLDER DATA (see Requirements 3 & 4)			**Responsible Party**
Requirement 3:	**Protect stored cardholder data**		**CaTS & Academic/Administrative Depts.**
	Overview	Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, with 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 the full Primary Account Number (PAN) is not needed and not sending PAN in unencrypted e-mails.	
	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.	
	3.2	Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data encoded within the magnetic stripe of the card and the three or four digit card-validation code.	
	3.3	Mask PAN when displayed.	
	3.4	Render PAN, at a minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches: Strong one-way hash functions (hashed indexes), truncation, Index Tokens and securely stored pads, and strong cryptography with associated key management processes and procedures. The MINIMUM account information that must be rendered unreadable is the PAN.	
	3.5	Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.	
	3.6	Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data.	
Requirement 4:	**Encrypt transmission of cardholder data across open, public networks**		**CaTS & Academic/Administrative Depts.**
	Overview	Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.	
	4.1	Use strong cryptography and security protocols such as Secure Sockets (SSL) / Transport Layer Security (TLS) and Internet Protocol Security (IPSEC) 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, Wi-Fi, and Global System for Mobile communications (GSM), and General Packet Radio service (GPRS). For new wireless implementations, it is prohibited to implement Wired Equivalent Privacy (WEP) after March 21, 2009 and for current applications, WEP is prohibited to use after June 30, 2010.	
	4.2	Never send unencrypted PANs by e-mail or other end user messaging technologies.	
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM (see Requirements 5 & 6)			**Responsible Party**
Requirement 5:	**Use and regularly update anti-virus software or programs**		**CaTS**
	Overview	Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from malicious software	
	5.1	Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).	

	5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	
Requirement 6:	**Develop and maintain secure systems and applications**		**CaTS & Academic/Administrative Depts.**
	Overview	Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. . Secure coding practices for developing payments applications, change control procedures and other secure software development practices should always be followed.	
	6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	
	6.2	Establish a process to identify newly discovered security vulnerabilities such as subscribing to alert services, or using a vulnerability scanning service or software. Update the process to address new vulnerability issues.	**CaTS**
	6.3	Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.	
	6.4	Follow change control procedures for all system and software configuration changes. The procedures must include documentation of impact, management sign-off by appropriate parties, testing of operational functionality, and back-out procedures.	
	6.5	Develop all Web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes to include unvalidated input, broken access control, broken authentication and session management, cross-site scripting attacks, buffer overflows, and injection flaws.	
	6.6	Ensure that all public Web-facing applications are protected against known attacks with at least annual reviews of and by installing a Web application firewall in front of public-facing Web applications.	
IMPLEMENT STRONG ACCESS CONTROL MEASURES (see Requirements 7, 8, & 9)			**Responsible Party**
Requirement 7:	**Restrict access to cardholder data by business need-to-know**		**CaTS & Academic/Administrative Depts.**
	Overview	This requirement ensures critical data can only be accessed by authorized personnel.	
	7.1	Limit access to system components and cardholder information only to those individuals whose job requires such access.	
	7.2	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.	
Requirement 8:	**Assign a unique ID to each person with computer access**		**CaTS & Academic/Administrative Depts.**
	Overview	Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.	

	8.1	Assign all users with a unique user name before allowing them to access system components or cardholder data.	
	8.2	Employ at least one of these to authenticate all users: Password or Passphrase; or two-factor authentication (e.g., token devices smart cards, biometrics, and public keys).	
	8.3	Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or Virtual Private Network with individual certificates.	
	8.4.	Render all passwords unreadable for all system components both in storage and during transmission using strong cryptography based on approved standards.	
	8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	
		1. Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	
		2. Verify user identity before performing password resets.	
		3. Set first-time passwords to a unique value for each user and change immediately after the first use.	
		4. Immediately revoke access for any terminated users.	
		5. Remove inactive user accounts at least every 90 days.	
		6. Enable accounts used by vendors for remote maintenance only during the time period needed.	
		7. Communicate password procedures and policies to all users who have access to cardholder data.	
		8. Do not use group, shared, or generic accounts and passwords.	
		9. Change user passwords at least every 90 days.	
		10. Require a minimum password length of at least seven characters.	
		11. Use passwords containing both numeric and alphabetic characters.	
		12. Do not allow an individual to submit a new password that is the same as any of the last four passwords s/he has used.	
		13. Limit repeated access attempts by locking out the user ID after not more than six attempts.	
		14. Set the lockout duration to thirty minutes or until administrator enables the user ID.	
		15. If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.	
		16. Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	
Requirement 9:	**Restrict physical access to cardholder data**		

			CaTS & Academic/Administrative Depts.
	Overview	Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted.	
	9.1	Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.	
	9.2	Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. (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).	
	9.3	Ensure all visitors are handled as follows:	
		1. Authorized before entering areas where cardholder data is processed or maintained.	
		2. Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees.	
		3. Asked to surrender the physical token before leaving the facility or at the date of expiration.	
	9.4	Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.	
	9.5	Store media backups in a secure location, preferably in an off-site facility.	
	9.6	Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data.	
	9.7	Maintain and strict control over the internal or external distribution of any kind of media that contains cardholder data including classifying the media so it can be identified as confidential and sending the media by secured courier or other delivery method that can be accurately tracked.	
	9.8	Ensure management approves any and all media containing cardholder data moved from a secured area (especially when media is distributed to individuals).	
	9.9	Maintain strict control over the storage and accessibility of media that contains cardholder data.	
	9.10	Destroy media containing cardholder data when it is no longer needed for business or legal reasons including cross-cut shred, incinerate, or pulp hardcopy materials and/or purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.	
REGULARLY MONITOR AND TEST NETWORKS (see Requirements 10 & 11)			**Responsible Party**
Requirement 10:	**Track and monitor all access to network resources and cardholder data**		**CaTS**
	Overview	Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something does go wrong.	

		Determining the cause of a compromise is very difficult without system activity logs.	
	10.1	Establish a process for linking all access to system components each individual user –especially access done with administrative privileges.	
	10.2	Implement automated audit trails for all system components to reconstruct the following events:	
		1. All individual user accesses to cardholder data.	
		2. All actions taken by any individual with root or administrative privileges.	
		3. Access to all audit trails.	
		4. Invalid logical access attempts.	
		5. Use of identification and authentication mechanisms.	
		6. Initialization of the audit logs.	
		7. Creation and deletion of system-level objects.	
	10.3	Record at least the following audit trail entries for all system components for each event:	
		1. User identification	
		2. Type of event	
		3. Date and time	
		4. Success or failure indication	
		5. Origination of event	
		6. Identify or name of affected data, system component, or resource.	
	10.4	Synchronized all critical system clocks and times.	
	10.5	Secure audit trails so they cannot be altered.	
		1. Limit viewing of audit trails to those with a job-related need.	
		2. Protect audit trail files from unauthorized modifications.	
		3. Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	
		4. Copy logs for wireless networks onto a log server on the internal LAN.	
		5. Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	
	10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion, detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note- log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.	
	10.7	Retain audit trail history for at least one year; at least three	

		months of history must be immediately available for analysis.	
Requirement 11:	**Regularly test security systems and processes**		**CaTS**
	Overview	Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.	
	11.1	Test for the presence of wireless access points by using a wireless analyzer at least quarterly , or deploying a wireless IDS/IPS to identify all wireless devices in use.	
	11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). 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 organization's internal staff.	
	11.3	Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment. These penetration tests must include network-layer and application-layer penetration tests.	
	11.4	Use network intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	
	11.5	Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly. Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).	
MAINTAIN AN INFORMATION SECURITY POLICY (see Requirement 12)			**Responsible Party**
Requirement 12:	**Maintain a policy that addresses information security for employees and contractors**		**CaTS**
	Overview	A strong security policy sets the security tone for the whole organization and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.	
	12.1	Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements includes an annual process for identifying vulnerabilities and formally assessing risks, and includes a review at least once a year and when the environment changes	
	12.2	Develop daily operational security procedures that are consistent with requirements in PCI DSS.	
	12.3	Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper	

		use of these technologies for all employees and contractors. Ensure these usage policies require the following:	
		1. Explicit management approval.	
		2. Authentication for use of the technology.	
		3. List of all such devices and personnel with access.	
		4. Labeling of devices with owner, contact information, and purpose.	
		5. Acceptable uses of the technologies.	
		6. Acceptable network locations for the technologies.	
		7. List of organization approved products.	
		8. Automatic disconnect of modem sessions after a specific period of inactivity.	
		9. Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.	
		10. When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access.	
	12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	
	12.5	Assign to an individual or team the following information security management responsibilities:	
		1. Establish, document, and distribute security policies and procedures.	
		2. Monitor and analyze security alerts and information, and distribute to appropriate personnel.	
		3. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	
		4. Administer user accounts, including additions, deletions, and modifications.	
		5. Monitor and control all access to data.	
	12.6	Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.	
		1. Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions).	
		2. Require employees to acknowledge in writing that they have read and understood the organization's security policy and procedures.	
	12.7	Screen potential employees prior to hire to minimize the risk of attacks from internal sources. Inquire with Human Resources and verify that background checks are conducted (within the constraints of local law) on employees prior to hire who will have access to cardholder data or the cardholder data	**CaTS & Academic/Administrative Depts.**

		environment. (Examples of background checks include pre-employment, criminal, credit history, and reference checks.) 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.	
	12.8	If cardholder data is shared with service providers, then contractually the following is required:	
		1. Service providers must adhere to the PCI DSS requirements.	
		2. Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses.	
	12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach.	
		1. Create the incident response plan to be implemented in the event of system compromise.	
		2. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and the credit card associations).	
		3. Designate specific personnel to be available on a 24/7 basis to respond to alerts.	
		4. Provide appropriate training to staff with security breach response responsibilities.	
		5. Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	
		6. Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	
		7. Test the plan at least annually.	
			CaTS