Credit Card Security Policies

PCI DSS 2.0

Version 1.0 - July 30, 2013

Revision History

Changes	Approving Manager	Date
Initial Publication	Barb Sweeney	July 30th, 2013

Introduction and Scope

Introduction

This document explains Teachers' Treasures credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Teachers' Treasures management is committed to these security policies to protect information utilized by Teachers' Treasures in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Teachers' Tresures' cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C, ver. 2.0, October, 2010. Should Teachers' Treasures implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of Teachers' Treasures to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. 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. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

All open ports and services must be documented. Documentation should include the port or service, source and destination, and a business justification for opening said port or service. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized (PCI Requirement 1.3.5)
- Firewalls must implement stateful inspection, also known as dynamic packet filtering (PCI Requirement 1.3.6)

Any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are to access the organization's network must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to:

- default encryption keys
- passwords
- SNMP community strings
- default passwords/passphrases on access points
- other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption for authentication and transmission of data over wireless networks. (PCI Requirement 2.1.1)

Unneeded Services and Protocols

Only necessary services, protocols, daemons, etc., as needed for the function of the system may be enabled. All services and protocols not directly needed to perform the device's specified function must be disabled. (PCI Requirement 2.2.2)

Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must include administrator access to web-based management interfaces

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

ABC Corporation will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols (e.g., IPSEC, SSLTLS). Only trusted keys and/or certificates can be accepted. For SSL/TLS implementations HTTPS must appear as part of the URL, and cardholder data may only be entered when HTTPS appears in the URL. (PCI Requirement 4.1)

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: use and Regularly Update Anti-Virus Software or Programs

Anti-Virus

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and capable of generating audit logs. Anti-virus logs must be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Requirement 6: Develop and Maintain Secure Systems and Applications

Security Patches

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. (PCI Requirement 6.1)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to ABC Corporation's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.1)

Privileges must be assigned to individuals based on job classification and function (also called "role-based access control). (PCI Requirement 7.1.2)

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (PCI Requirement 8.3)

Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.5.6)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.6)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include:

> Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.7.1)
>
> Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.7.2)

Logs must be maintained to track all media that is moved from a secured area, and management approval must be obtained prior to moving the media. (PCI Requirement 9.8)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.9)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Container storing information waiting to be destroyed must be secured to prevent access to the contents. (PCI requirement 9.10.1)

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, ABC Corporation will perform testing to ensure there are no unauthorized wireless access points present in the cardholder environment. (PCI Requirement 11.1)

This testing must detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components
- Portable wireless devices connected to system components (for example, by USB, etc.)
- Wireless devices attached to a network port or network device

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.) it must be configured to generate alerts

Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.9).

Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), ABC Corporation will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be repeated until passing results are obtained, or until all "high" vulnerabilities as defined in PCI Requirement 6.2 are resolved. (PCI Requirement 11.2.1, 11.2.3)

Quarterly vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures. External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). (PCI Requirement 11.2.2, 11.2.3)

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

ABC Corporation shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.3)

Critical Technologies

ABC Corporation shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

Explicit approval by authorized parties to use the technologies (PCI Requirement 12.3.1)

Authentication for use of the technology (PCI Requirement 12.3.2)

A list of all such devices and personnel with access (PCI Requirement 12.3.3)

Acceptable uses of the technologies (PCI Requirement 12.3.5)

Acceptable network locations for the technologies (PCI Requirement 12.3.6)

Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity (PCI Requirement 12.3.8)

Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate de-activation after use (PCI Requirement 12.3.9)

Security Responsibilities

ABC Corporation's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

The Executive Director shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within

their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records

Reporting an Incident

The Executive Director should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the _Executive Director to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the Executive Director about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Executive Director.

Document any information you know while waiting for the Executive Director to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

MasterCard

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

Discover Card

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)

d. Local authorities (if appropriate)

3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm

4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Executive Diirector will work with legal and management to identify appropriate forensic specialists.

5. Eliminate the intruder's means of access and any related vulnerabilities.

6. Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Board of Directors and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

Teachers' Treasures shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Service Providers

Teachers' Treasures shall implement and maintain policies and procedures to manage service providers. (PCI requirement 12.8)

This process must include the following:

- ❑ Maintain a list of service providers (PCI requirement 12.8.1)
- ❑ Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (PCI requirement 12.8.2)
- ❑ Implement a process to perform proper due diligence prior to engaging a service provider (PCI requirement 12.8.3)
    - ❑ Monitor service providers' PCI DSS compliance status (PCI requirement 12.8.4)