School of Dentistry, University of Maryland

Credit Card Security Policies

PCI DSS 2.0

Version 1.0 - February, 18, 2014

Revision History

Changes	Approving Manager	Date
Initial Publication	**Kent Buckingham**	2-18-2014

HIPAA & IT Security Officer, School of Dentistry - Kent Buckingham
Chief Information Security Officer - Frederick W. Smith

Introduction and Scope

Introduction

This document explains School of Dentistry, University of Maryland's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. School of Dentistry, University of Maryland management is committed to these security policies to protect information utilized by School of Dentistry, University of Maryland 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, School of Dentistry, University of Maryland's cardholder environment consists only of imprint machines or standalone dial-out terminals. The environment 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) B, ver. 2.0, October, 2010. Should School of Dentistry, University of Maryland implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ B, it will be the responsibility of School of Dentistry, University of Maryland to determine the appropriate compliance criteria and implement additional policies and controls as needed.

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

School of Dentistry, University of Maryland 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

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

Limit Access to Cardholder Data

Access to School of Dentistry, University of Maryland'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 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 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

School of Dentistry, University of Maryland 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

School of Dentistry, University of Maryland 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)

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)

Security Responsibilities

School of Dentistry, University of Maryland's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

The IT Security Officer [A1] 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 IT Security Officer [A2] should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the IT Security Officer [A3] 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 IT Security Officer [A4] about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the IT Security Officer .[A5]

Document any information you know while waiting for the IT Security Officer [A6] 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 IT Security Officer [A7]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 IT Security Officer [A8]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

School of Dentistry, University of Maryland 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

School of Dentistry, University of Maryland 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)