What is PCI DSS and how does it affect me?

WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide security standard designed to ensure that all organizations that process, store, or transmit credit card information maintain a secure environment. This standard was created to protect cardholders against misuse of their personal information.

Per University policy, University units that accept payment cards (credit or debit) as a method of payment must protect cardholder information of students, parents, donors, alumni, customers, and any individual or entity that utilizes a credit card to transact business with the University. This includes meet University policy, state and federal laws, and contractual obligations to the University's banks and financial institutions (this includes adherence to the PCI DSS).

HOW DOES PCI DSS AFFECT ME?

Each department accepting payment cards is required to certify annually that they comply with the PCI DSS. This compliance includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent credit card fraud, hacking, and various other security vulnerabilities and threats. The complete PCI DSS requirements can be found on the PCI Security Standards Council website at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

University of Minnesota
Accounts Receivable Services
Controller's Office
West Bank Office Building
1300 S. 2nd Street
Minneapolis, MN 55454
(612) 625-2392
http://www.finsys.umn.edu/ar/biz_ar_pcidss.html

May 2014

This document is to be used for informational purposes only and does not supersede University policy or the PCI Data Security Standards.

Understanding PCI DSS COMPLIANCE

All University of Minnesota employees should always adhere to the highest standards when it comes to protecting sensitive data.

UNDERSTANDING THE HIGH VALUE OF SECURING FINANCIAL DATA IS ESSENTIAL.

HANDLING CARDHOLDER DATA (CHD)

All departments accepting credit cards must comply with the following security procedures relating to the handling of cardholder data (CHD):

1. You must not send or receive CHD by e-mail, chat, or instant messaging.
2. You must never store CHD in electronic format on any university computer or external device.
3. The card verification code (CVC) or value (CVV) must never be stored in any form after authorization.
4. You must retain any paper documents containing CHD only for as long as needed to complete the transaction.
5. Upon completion of the transaction, any paper documents containing CHD must be properly destroyed (cross-cut shredded).
6. Access to CHD must be limited to only those individuals whose jobs require access.

PCI DSS compliance is a collaborative effort among all the departments at the University of Minnesota. This collaboration of compliance provides many benefits to our University by making us aware of all sensitive consumer data, increasing the security of many processes by applying data security standards to other areas, allowing us to respond quickly to the dynamic world we live in, and maintaining consistent policies and procedures so that all departments feel secure in accepting credit and debit cards as a form of payment.

Non-compliance with the PCI Data Security Standards puts the University in a position of unnecessary risk for large monetary fines assessed to the University and/or your department, loss of merchant status for the University and/or your department, and loss of faith in the University of Minnesota name.

Ensuring compliance with PCI data security standards is up to all of us

SELF-ASSESSMENT QUESTIONAIRE (SAQ)

The SAQ is a self-validation tool which consists of two components: a set of yes-or-no questions about your security posture and practices corresponding to the PCI DSS requirements, and an Attestation of Compliance. The Attestation is certification that you have performed the appropriate self-assessment and that you are compliant with PCI Data Security Standards. Every merchant manager is required to complete an SAQ annually.

PCI DATA SECURITY STANDARDS TRAINING

All employees who handle cardholder data must complete applicable PCI DSS training requirements. For information on role-specific PCI DSS training offered by the University of Minnesota, visit the University's PCI DSS website at http://www.finsys.umn.edu/ar/biz_ar_pcidss.html.

Tips to help ensure compliance

HAVE APPROVED OPERATIONAL PROCEDURES IN PLACE

All departments that handle CHD are required to have approved operational procedures in place. These procedures are to be reviewed annually and updated as needed.

HAVE AN APPROVED INCIDENT RESPONSE PLAN IN PLACE

All departments that handle CHD are required to have an approved incident response plan in place. This plan is to be reviewed and tested annually.

CHANGE DEFAULT PASSWORDS

You are required to change default passwords on all routers, firewalls, software, etc. that exist in the CHD environment. This new password should be at least seven-character alphanumeric.

LABEL DEVICES

Devices that exist in the CHD environment need to be labeled to determine owner, contact information, and purpose.

USE AND UPDATE FIREWALLS AND ANTI-VIRUS SOFTWARE

Many vulnerabilities and viruses can enter the network via e-mail and online activities. Anti-virus software must be used on all systems in the cardholder data environment.