PCI DSS Security Awareness Program Standard for University of Tennessee and University of Tennessee Foundation Merchants

Revision: March 28, 2016

Purpose

To outline the University's formal security awareness program to make all personnel who are involved in the processing of credit card payments aware of the importance of cardholder data security as required by the Payment Card Industry Data Security Standards (PCI DSS).

Scope

This standard applies to all University of Tennessee system-wide merchants, as well as all University of Tennessee Foundation merchants.

Key Roles and Responsibilities

Merchant

- All merchant employees who process cardholder data must complete security awareness training upon hire, and at least annually.
- All merchant employees must regularly review the Security Awareness Information found on UT's PCI Compliance website at http://security.tennessee.edu/pci-dss-compliance-information/.
- All merchant employees must acknowledge in writing, or at least electronically, that they have read and have an understanding of the merchant's internal policies and procedures, as well as all UT policies and procedures regarding PCI.

Campus Chief Business Officer

- Sends security awareness flyers to UT merchants at least annually.

University of Tennessee Treasurer's Office

- Notifies UT merchants of PCI security alerts via UT's PCI listserv.
- Maintains UT's PCI listserv.

University of Tennessee Foundation Assistant VP of Finance and Operations

- Notifies UTFI merchants of PCI security alerts.
- Sends security awareness flyers to UTFI merchants at least annually.

University of Tennessee System Administration Information Security Office (UTSA ISO)

- Provides the security awareness training and maintains records of participation for UT and UTFI merchants.

- Maintains UT’s PCI Compliance website and the information available on that site.
- Notifies the Treasurer’s Office and UTFI’s Assistant Vice President of Finance and Operations when important PCI security alerts become available.
- Maintains the *PCI DSS Security Awareness Program Standard for University of Tennessee and University of Tennessee Foundation Merchants*.

Security Awareness Program Requirements for PCI v3.x

PCI DSS Requirement 12.6, and its sub-requirements require that merchants implement a formal security awareness program, making employees aware of the importance of cardholder data security. The security awareness program is a way to communicate with and educate all employees who process credit card payments. The security awareness program consists of multiple parts.

First, all employees processing cardholder data must complete the security awareness training upon hire and at least annually. Should a merchant supervisor notice questionable employee practices when processing credit card payments, the supervisor should ask that employee to retake the training to ensure a proper understanding of the material.

The security awareness program must also provide multiple means of communicating awareness to merchant employees. UT and UTFI merchants will be sent security awareness flyers at least annually. The flyers should be posted in an area available to all employees and those employees should be asked to review the flyers upon hire and at least annually.

The UTSA ISO will notify the Treasurer’s Office and UTFI Assistant Vice President of Finance and Operations of any security alerts. They will in turn disperse this information to their merchants.

Lastly, the merchant must maintain internal security policies and procedures. Each employee must review these policies and procedures, as well as UT’s PCI-related policies and procedures, upon hire and at least annually. All employees must, at least annually, provide some form of written acknowledgement that they have read and understood these policies.

Definitions

- Cardholder – The customer to whom a payment card is issued or an individual authorized to use the payment card is known as the cardholder.
- Cardholder Data (CHD) – Cardholder data is any personally identifiable data associated with a cardholder's account. At a minimum, CHD consists of the full primary account number (PAN), but may also consist of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.
- Merchant's Internal Documentation – PCI DSS requires that merchants document many specific policies and procedures for processing, storing, and transmitting cardholder data. Many of the internal policies and procedures are documented, for your convenience, in the PCI DSS Internal Policies and Procedures template found on UT's PCI Compliance website at http://security.tennessee.edu/pci-dss-compliance-information/. Please add your own departmental information where highlighted.
- UT or UTFI Merchant – A UT or UTFI department/office/organization that collects payments, electronically or manually, via payment card OR is otherwise involved in storing, processing, transmitting, or receiving payment card or cardholder data.