UTIA IT0311 – PAYMENT CARD INDUSTRY (PCI) SECURITY PLAN

Effective: February 20, 2017
Last Reviewed: May 08, 2018 **Last Updated:** February 08, 2017

Objective:
This plan, in accordance with UT Policy FI0311 – *Credit Card Processing*, addresses the requirements and guidelines for accepting and processing credit card transactions by any University of Tennessee Institute of Agriculture (the Institute) merchant. These requirements and guidelines are based on the Payment Card Industry Data Security Standards (PCI DSS).

Scope:
This plan applies to all employees who process and/or transmit credit card, debit card, or eCommerce transactions on behalf of an Institute merchant. Such employees will be collectively referred to in this document as "the merchant." Compliance with the PCI DSS requirements, UT Policy FI0311, and the UTIA IT0311 – *Payment Card Industry (PCI) Security Plan* is mandatory for all Institute merchants.

Policies:
Protection of Cardholder Data – General

1. The merchant must verify that all employees who handle cardholder data have received annual training given by the Institute's Chief Information Security Officer (CISO).
2. Vendor-supplied defaults (i.e., passwords, services, etc.) must be changed and all unnecessary default accounts must be disabled prior to installing any Institute IT asset on the network.
3. Each merchant employee accessing Institute IT assets and/or cardholder data must be assigned a unique ID and authentication method.
    a. The unique ID must be immediately disabled for any user who is terminated or will no longer require such access.
    b. Authentication will use one or more of the following methods:
        - Something you know (i.e., password or passphrase)
        - Something you have (i.e., token or smartcard)
        - Something you are (i.e., biometric)
    c. When a password is used, it must contain at least seven characters and must include both numeric and alphabetic characters.
4. Generic or group accounts are prohibited.
5. Cardholder data must be restricted to merchant employees on a need-to-know basis.
    a. Access rights are granted to privileged users to the least privileges necessary to perform job responsibilities.

    b. The privileges will be assigned based on role-based access control (i.e., job classification and function).
6. Strict control of all media pertaining to credit card processing is maintained at all times with regards to internal or external distribution of media.
    a. All media, including but not limited to, computers, point-of-sale terminals, other removable electronic media, paper receipts, paper reports, and faxes, is classified as moderate and will be secured as such.
    b. Media leaving the merchant area will be sent via secured courier or other delivery method that can be accurately tracked, and management will approve by signature prior to moving it.
    c. All reports and receipts with cardholder information are secured in a locked cabinet with limited access.
    d. After transactions have been approved via Elavon, the receipt has been printed, and documentation is no longer needed for business or legal reasons (see UT Policy FI120 – *Records Management*) all card numbers and personal information are shredded using a cross-cut shredder so that the media cannot be reconstructed.
    e. If shredding is not done on site, a secured storage container (i.e., locked bin provided by a reputable shredding company) will be used to prevent access to the contents.
    f. The merchant must maintain internal procedures detailing how paper and electronic records are destroyed (e.g., Records Management, Shred-It, etc.).
7. Only approved critical technologies (i.e., POS devices and web applications) are allowed and users are required to have complete understanding and acknowledgement of their proper and acceptable uses prior to the necessary explicit authorization by management.
8. PCI device inventory logs are maintained to provide strict control of storage and accessibility.
    a. The inventory list includes the make, model, location, and the explicitly authorized users of the device.
    b. The inventory list is updated when IT assets are added, relocated, decommissioned, or when authorized users change.
9. Never store cardholder data electronically.
10. Never send cardholder data via text, chat, or other end-user messaging technologies.
11. Never ask for or accept credit card payments via email.
    a. Should a customer email their card information to a merchant representative, the email must be deleted immediately and the email Deleted Items/Trash must be immediately emptied.
    b. The customer must be sent a new email (not a reply to the original message) saying that the email containing credit card information has been deleted and payments cannot be accepted via email; and the customer will be given alternative methods for making payments. All sensitive authentication data must be deleted or rendered unrecoverable (e.g., redacted) upon completion of the authorization process.

12. The merchant must not retain the full content of any track from the card's magnetic stripe, the personal identification number (PIN), or encrypted block once the transaction has been authorized.
13. Under no circumstances shall the merchant ever store the card verification code (CVC, CVV).
14. The Primary Account Number (PAN) must be masked and only the last four digits can be displayed on any printed materials or credit card devices, including reports and receipts.
15. Leaving media of any kind unsecured for viewing, scanning, or copying is strictly prohibited.
16. In the event of any suspected data breach, the merchant must immediately contact the Institute's CISO.
    a. Do not turn the computer off.
    b. Do not make changes to the computer.

<u>Protection of Cardholder Data – Point-of-Sale (POS) Transactions</u>

1. The merchant must process all POS transactions using only an approved POS device.
    a. POS devices must be purchased from Elavon through the University of Tennessee Treasurer's Office.
    b. POS devices must be used only for processing the merchant's credit card transactions, as other uses are considered unacceptable.
    c. The use of devices such as Square is strictly prohibited.
2. The merchant must properly maintain and update the POS device according to Elavon's guidelines to ensure the device remains compliant.
3. The merchant must secure any POS device(s) in a locked cabinet or office, and must detail the procedures for securing such devices in the merchant's internal procedures document.
4. The merchant must periodically inspect the POS device(s) for tampering and substitution, including, but not limited to verification of serial number and review of unapproved attachments or cables.
5. The merchant must verify that all employees who handle cardholder data have received training given by the Institute's CISO prior to using any POS device.
    a. This training must include information on privacy and confidentiality.
    b. This training must also address how to be aware of and identify tampering of POS.
6. The merchant must ensure that the proper background checks have been done when hiring employees who will process and/or transmit credit card transactions.

<u>Protection of Cardholder Data – Internet Sales Transactions</u>

1. The merchant must ensure all transactions are securely processed by using TouchNet as the payment gateway, as TouchNet is the only UT-approved gateway.
2. TouchNet must process transactions over a connection using a protocol for encrypting information over the Internet; SSL/TLS older than v1.1, must not be used.

3. The merchant must maintain internal procedures detailing where cardholder data resides and how it is protected.
4. The merchant must never enter cardholder data for the customer/client/donor.
5. The merchant must never instruct a customer/client/donor to use any UT-owned asset (i.e., merchant computer, lab computer, library computer, etc.) on the UT-owned network for making credit card payments for Institute products and services.

Protection of Cardholder Data – Web-based Virtual Payment Terminals

1. The system administrator for the merchant's IT assets must create a firewall, router, and system configuration standards document.
    a. This document must include details of all firewall, router, and system configurations necessary to meet the PCI DSS requirements.
    b. The standards document must also contain the specific procedures for implementing the standards.
2. Firewall and router configurations must restrict connections between untrusted networks and any IT asset in the cardholder data environment (CDE).
3. The University's WiFi network must not be used when processing credit card transactions.
4. Direct public access must be prohibited between the Internet and any system component in the CDE.
5. Vendor-supplied defaults (i.e., passwords, services, etc.) must be changed and all unnecessary default accounts must be disabled prior to installing an IT asset on the network.
6. Only necessary services, protocols, daemons, etc., must be enabled as required for the function of the system; otherwise, the merchant must provide documented business justification.
7. Additional security features must be documented and implemented for any required services, protocols, or daemons considered to be insecure.
8. The use of SSL/early TLS is strictly prohibited.
9. Strong cryptography and security protocols must be used to safeguard sensitive cardholder data during transmission over open, public networks.
10. Antivirus software must be deployed on all IT assets used for processing credit card transactions.
    a. The merchant must use reputable antivirus software capable of detecting, removing and protecting against all known tapes of malware.
    b. The antivirus software must be updated and maintained, getting latest software and definitions updates.
    c. Antivirus mechanisms must be actively running and configured such that users cannot disable or alter.
    d. Automatic updates and regular scans must be performed.
        i. Audit logs must be retained for at least one year.

ii. At least three months of log history must be immediately available for analysis.

11. The University uses a classification process for primary users of IT assets to state what type of data is on an Institute IT asset.
    a. This process must be used, in part, to identify IT assets processing credit card transactions.
    b. IT assets used to process credit card payments are classified as moderate.
12. All Institute IT assets classified as moderate must be included in the monthly scanning process, per the UTIA IT0124P2 – *Vulnerability Assessment Procedures*.
13. All vendor-supplied patches and critical security patches must be installed within one month of release.
14. The merchant must use multi-factor authentication for all non-console administrative access and all remote access to the CDE.
    a. Multi-factor authentication must be used for all non-console access into the CDE for personnel with administrative access.
    b. Authentication will use at least two of the following methods:
        - Something you know (i.e., password or passphrase)
        - Something you have (i.e., token or smartcard)
        - Something you are (i.e., biometric)
    c. Group or generic accounts are prohibited.
    d. Shared accounts and shared passwords are prohibited.
15. Physical controls must be put in place to limit and monitor physical access to IT assets in the CDE.
16. Network segmentation must be used to isolate the CDE from other networks.
    a. Penetration-testing procedures must be defined for testing all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

Merchant Responsibilities

1. Responsible for implementing these policies, as well as all internal procedures, and must regularly discuss with all relevant personnel to ensure a clear understanding of policies and procedures.
2. Use only Elavon as the processor and TouchNet as the payment gateway.
    a. Written agreements with these providers, which includes responsibilities of the provider, are maintained by the Treasurer's Office.
    b. Prior to initiating service requests with service providers, contact the Treasurer's Office.
    c. Annual PCI DSS compliance status for these providers may be obtained through the Treasurer's Office or through the PCI Security Standards Council website for Validated Payment Applications.
3. Discuss possible use of any third-party service provider with the Institute's CISO and the Institute's Chief Business Officer (CBO) prior to speaking with vendors.

4. Stay involved in the Institute's security awareness program.
5. Complete the *UTIA Merchant Process Change Request Form* prior to making changes to any part of the processes associated with the original Merchant ID (MID) for which it was approved. This form must be discussed with, and approved by, the unit's Budget Director, as well as the Institute's CISO and CBO.
6. Must discuss plans for applying for a new MID with the unit's Budget Director, as well as the Institute's CISO and CBO to ensure feasibility and security. The prospective merchant must then complete the *Point-of-Sale and Internet Sales Approval Form for Departments*, which must then be approved by the Institute's CISO and CBO, then sent to the Treasurer's Office for processing.
7. Complete the appropriate annual Self-Assessment Questionnaire for each MID the merchant owns.
8. Comply with all requirements and responsibilities in UT and Institute PCI policies.

Institute CISO Responsibilities

1. Regularly review and maintain the UTIA IT0311 – *Payment Card Industry (PCI) Security Plan*, updating as needed.
2. Publish the UTIA IT0311 – *Payment Card Industry (PCI) Security Plan* on the Institute's IT Security Site, giving access to merchants.
3. Maintain the Institute's formal security awareness plan. (See UTIA IT0123 – *Security Awareness, Training, and Education Plan*.)
4. Provide technical guidance for the merchants.
5. Provide annual PCI training to the merchants.
6. Provide annual PCI assessment to certify PCI compliance for each merchant.
7. Review, verify, and approve all PCI-related documentation before submitting to the Institute's CBO.
8. Notify UT System Administration CISO of any suspected security breaches prior to making any changes to any PCI devices. (See UTIA IT0122 – *Information Security Incident Response Plan* and UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*.)
9. Meet all responsibilities in UT Policy FI0311 – *Credit Card Processing*.

Institute CBO Responsibilities

1. Approve business need for any prospective merchants requesting to accept credit cards.
2. Review and approve (or deny) changes to any existing merchant processes.
3. Approve all PCI-related documentation before submitting to the Treasurer's Office.
4. Meet all responsibilities in UT Policy FI0311 – *Credit Card Processing*.

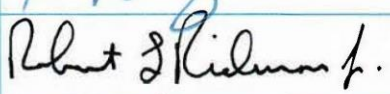
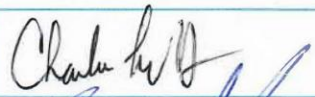
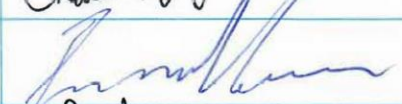
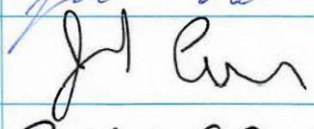
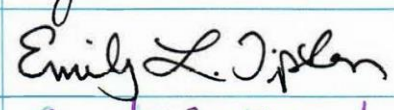
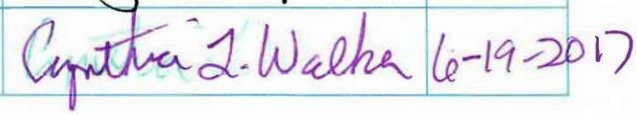
References:

UTIA Glossary of Information Technology Terms
UT Policy FI0311 – *Credit Card Processing*
UTIA Internal PCI Procedures Template
UTIA PCI Point-of-Sale (POS) Device Inspection List
UTIA PCI DSS Inventory Log
UTIA Merchant Process Change Request Form
Point-of-Sale and Internet Sales Approval Form for Departments
UT Policy FI0120 – *Records Management*
UTIA IT0122 – Information *Security Incident Response Plan*
UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*
UTIA IT0312 – *Payment Card Industry (PCI) Security Awareness Program*
UTIA IT0123 – *Security Awareness, Training, and Education Plan*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)*

For more information, contact Sandy Lindsey, CISO, at (865) 974-7292, or email sandy@tennessee.edu.

Approval of Plan

We approve the UTIA IT0311 – *Payment Card Industry (PCI) Security Plan* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		06/16/2017
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		6/16/2017
Charles Lambrecht	Computer Operations Manager, UTCVM		6/16/17
Brent Lamons	Director of Advising, Herbert College of Agriculture		6/19/17
Joel Lown	Coordinator, AgResearch		6/16/17
Emily Tipton	IT Coordinator, Extension		6/16/17
Cynthia Walker	IT Administrator, Plant Sciences		6-19-2017