Objective:
This program is designed for the University of Tennessee Institute of Agriculture (UTIA or Institute) to meet the Payment Card Industry Data Security Standard (PCI DSS) requirements for a formal security awareness program to make personnel aware of cardholder data security.

Scope:
This program applies to all employees, including students, who process and/or transmit credit card, debit card, or eCommerce transactions on behalf of an Institute merchant.

Program:
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.

All merchant 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. Institute 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.

Lastly, the merchant must maintain internal security procedures specific to their own processes. Each employee must review these procedures, as well as the UTIA IT0311 – Payment Card Industry (PCI) Security Plan and UT's PCI-related policies, plans, and procedures, upon hire and at least annually. All applicable employees must annually provide some form of written or emailed attestation that they have read and understood these policies. This attestation must be given to the merchant Primary Point of Contact to file (electronically or otherwise) and be provided to the Institute's Chief Information Security Officer (UTIA CISO), UT's Treasurer's Office, auditor, or PCI official when asked.

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 the PCI section of the Institute's IT security website.
- All merchant employees must acknowledge in writing, or at least electronically, that they have read and understand the merchant's internal policies and procedures, as well as all UTIA and UT policies and procedures regarding PCI.

UTIA Chief Information Security Officer
- Ensures annual PCI training offered by UT System Administration is completed by all merchant employees who process cardholder data.
- Maintains records of PCI training participation.
- Notifies Institute merchants of security alerts.
- Maintains UTIA_PCI email group.
- Sends PCI security awareness flyers at least annually.
- Maintains the Institute's IT security website, which includes a section on PCI.

References:
UTIA Glossary of Information Technology Terms
UTIA IT0311 – Payment Card Industry (PCI) Security Plan
UTIA Policy FI0311 – Credit Card Processing
UTIA Internal Credit/Debit Card Processing Procedures

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

Approval of Program

We approve UTIA IT0312 – Payment Card Industry (PCI) Security Awareness Program as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Senior Vice President and Senior Vice Chancellor, UTIA	*Tim Cross*	3/16/2020
Angela A. Gibson	Chief Information Officer, UTIA	*Angela A Gibson*	3/20/2020
Sandra D. Lindsey	Chief Information Security Officer, UTIA	*signature*	03/20/2020