College of Agricultural Sciences --- ePay Services Policy: ITP-006

1.0 Purpose

The purpose of this policy is to describe the process for granting user access to the university ePAY environment, and compliance with Payment Card Industry/Data Security Standards (PCI/DSS) and college and university security policies.

2.0 Scope

This policy applies to access privileges and PCI/DSS secure access services for employees, networks, and units in the College of Agricultural Sciences.

3.0 Policy

Individuals and their respective business unit who process and transmit cardholder information using the university ePay system must comply with PCI/DSS, university and college policies (refer to College policy ITP-008 *Credit Card Processing Privileges,* University policy AD 20 *Computer and Network Security,* and university policy FN 07 *Credit Card Sales*.) Credit card processing must be approved by the college Office of Administrative Services (OAS) and transacted within a secure IT environment managed by AgIT.

4.0 Account setup and user access

New credit card processing accounts, new user accounts, and changes to existing user accounts (deleting an account, or changing a users access from one business unit to another) are managed under the following guidelines:

New credit card processing account

1. The unit leader (or their designee) contacts the college business office requesting a new credit card processing account. The requesting unit submits a request form found at: http://adminsvcs.cas.psu.edu/
2. The college (OAS) will submit a request to AgIT to setup the secure card processing IT infrastructure. Ag IT will:
    a. Create or verify the existence of a secure credit card processing network at the user's location. This process includes the installation of a network firewall if one does not exist and may warrant the installation of additional Ethernet ports for the card processing workstation and an additional network card on the user workstation.
3. The process will continue with the guidelines for New user account or Changes to an existing account as appropriate.

New user account

1. The unit leader (or their designee) contacts the college OAS requesting a new user be granted credit card processing privileges. The requesting unit submits a request form found at: http://adminsvcs.cas.psu.edu/ .
2. The college OAS will submit a request to AgIT to setup the secure card processing IT infrastructure. Ag IT will:
    - Create or verify the existence of a secure credit card processing network at the user's location. This process includes the installation of a network firewall if one does not exist and may warrant the installation of additional ethernet ports for the card processing workstation.
    - Configure the user's desktop computer for a secure credit card processing environment. This includes the installation of a second network card and installation of credit card processing software on the user's computer.
    - Notify the college OAS of the IP address of the card processing computer.
4. The new user completes the PCI DSS Training Module and scores 70% or higher on the PCI DSS General User Quiz. Instructions for the training and quiz will be sent to the user when the credit card processing request form is received by the college OAS. The new user will also read and sign acknowledgement of the college's Credit Card Processing Privileges Policy ITP-008.

5. Upon notification of successful completion of the PCI DSS General User quiz, the Office OAS will finalize the account setup with the university eCommerce office, and notify the user that they may begin processing credit cards in the approved environment.

Changes to existing user account – account deletion

1. The unit leader (or their designee) contacts the college OAS requesting that card processing privileges be removed for a particular user. The requesting unit submits a request form found at: http://adminsvcs.cas.psu.edu/.
2. The college OAS will submit a request to AgIT to delete the user's access to the card processing environment on their workstation. Ag IT will delete the user's access to the card processing software.
3. The college OAS will notify the university eCommerce office to remove the user account and computer IP address from the ePAY authorization tables.

Changes to existing user account – changing a user's access from one business unit to another (user with existing card processing privileges)

1. The unit leader (or their designee) of the unit the user is transferring *to* contacts the college OAS requesting a user be granted credit card processing privileges. The requesting unit submits a request form found at: http://adminsvcs.cas.psu.edu/ .
2. The college OAS will submit a request to AgIT to setup the secure card processing IT infrastructure. Ag IT will:
    a. Create or verify the existence of a secure credit card processing network at the user's location. This process includes the installation of a network firewall if one does not exist.
    b. Configure the user's desktop computer for a secure credit card processing environment. This may include the installation of a second network card and installation of credit card processing software on the user's computer.
    c. Notify the OAS of the IP address of the card processing computer.
    d. NOTE: If the user will inherit a workstation previously used for card processing, AgIT will wipe the workstation and perform a clean install of the card processing software.
3. The OAS will finalize the account setup with the university eCommerce office, and notify the user that they may begin processing credit cards in the approved environment.
4. The unit leader (or their designee) of the unit the user is transferring *from* contacts the college OAS requesting that card processing privileges for that user be removed for the workstation on their network. The requesting unit submits a request form found at: http://adminsvcs.cas.psu.edu/. NOTE: steps 1 and 4 should be initiated at the same time.
5. The college OAS will submit a request to AgIT to delete the user's access to the card processing environment on the workstation in their former unit. AgIT will delete the users' access to the card processing software on the workstation in their former unit.

5.0 Supporting Documents

College policy ITP-001 CAS Acceptable Computer Use Policy
College policy ITP-008 Credit Card Processing Privileges
University policy AD 20 Computer and Network Security
University policy FN 07 Credit Card Sales

6.0 Revision History

Last updated: 1/5/2010