College of Agricultural Sciences --- Credit Card Processing Privileges Policy: ITP-008

1.0 Purpose

The purpose of this policy is to describe the responsibilities of college employees who are granted credit card processing privileges .

2.0 Scope

This policy addresses the responsibilities and practices of individuals who process credit card transactions in the College of Agricultural Sciences.

3.0 Policy

Individuals who process and transmit credit cardholder information for college business transactions are subject to the provisions set forth by the Payment Card Industry (PCI/DSS), and all relevant college and university policies including, but not limited to: university policy AD 20 *Computer and Network Security,* university policy FN 07 *Credit Card Sales*, university policy AD23 *Use of Institutional Data,* as well as the Required Business Practices described in section 4.0 of this document. Credit card processing is a privilege and brings a high level of trust and responsibility. Any individual processing credit card information must be approved by the college Office of Administrative Services and electronic processing must be transacted within a secure IT environment managed by AgIT.

4.0 Required Business Practices

The following business and operational practices are REQUIRED of individuals processing credit card information:

1. Only employees who have a legitimate business “need-to-know” should have access to cardholder information.
2. Employees with card processing privileges will complete the PCI/DSS training exam yearly.
3. Access account password must be changed every 90 days.
4. Sanitize credit card numbers on any document where the complete number is visible.
    a. Blackout credit card number (first 12 digits) and then photocopy.
    b. Shred the original, retain the copy.
    c. Cut out/off and shred card information.
5. Do not use wireless networks for the processing of Credit Cards.
6. Do not store credit card information online.
7. Maintain all software, OS updates and virus signatures. Users will open the ACE client on card processing workstations at least weekly to ensure all software updates are installed.
8. Only retain information long enough to reconcile payments.
9. Shred documentation containing credit card information when it is no longer needed for business or legal reasons.
10. Lock computer terminals and paper storage areas when un-attended. NEVER e-mail credit card information.
11. Protect computer networks with hardware firewall and intrusion detection/protection.
    a. Separate and encrypt credit card processing traffic from regular traffic.
    b. Limit Internet usage on computers that process credit cards.
12. Never e-mail credit card information.
13. Credit card processing may only be conducted using the university ePay system or the college Cvent application.

5.0 Supporting Documents

College policy ITP-001 CAS Acceptable Use Policy
College policy ITP-002 CAS Password Policy
University policy AD 20 Computer and Network Security

University policy FN 07 Credit Card Sales

6.0 Revision History

Last updated: 1/8/2010

7.0 Employee’s Confirmation

I have read, understand, and agree to comply with the provisions set forth in this policy.

____ ___________________
Signature Date

____ ___________________
Name (Please Print) PSU Access Account