Texas A&M AgriLife Research Procedures

21.01.02.A0.01 | Credit Card Collections

Approved: December 12, 2014

Next Scheduled Review: December 12, 2019

PROCEDURE STATEMENT

Texas A&M AgriLife Research (AgriLife Research) offers departments the convenience of accepting credit cards as payment for goods and services provided. Departments may accept credit card payments over the counter, over the telephone, through the mail, or over the internet.

REASON FOR PROCEDURE

This procedure outlines guidelines and responsibilities associated with acceptance of credit cards as payment for goods and services provided.

PROCEDURES AND RESPONSIBILITIES

1.0 RESPONSIBILITIES

1.1 AgriLife Fiscal

A. AgriLife Fiscal is responsible for administering the AgriLife Research credit card program, and for ensuring that participating departments are provided updates on all policies, regulations, rules, procedures, and security standards.

B. AgriLife Fiscal will:

- coordinate with the merchant bank on the merchant's behalf including cases of a suspected security breach;
- distribute and coordinate the preparation of the annual *Payment Card Industry Data Security Standards* (PCI DSS) questionnaire by each merchant;
- work closely with both the merchant and AgriLife Information Technology (AIT) to ensure that all necessary security procedures are in the protection of sensitive credit card data; and
- assess service charges to merchant department accounts for credit card transactions based on information supplied by Visa/MasterCard, and Discover.

1.2 AIT Network Security

A. AIT Network Security is responsible for approving the configuration of merchant's PCI computer systems.

B. AIT Network Security will perform vulnerability scans of PCI computer systems, and will require configuration changes to eliminate vulnerabilities in accordance with AgriLife Research procedure 29.01.99.A0.03, *AgriLife Research Network Procedures*. This is in preparation for and in addition to vendor scans that are required for PCI compliance. Vulnerabilities must be mitigated as soon as practical. In order to meet security needs, the AgriLife IT Group standards may be stricter than the PCI requirements.

1.3 Departments/Units

A. Departments/units participating in the credit card program are responsible for complying with all policies, regulations, rules, and procedures issued by the Texas A&M University System (System) and AgriLife Research, as well as with all PCI DSS, including periodic business review and completion of the annual PCI questionnaire.

B. Departments/units will provide any reasonable assistance necessary to AgriLife Fiscal in the performance of periodic reviews of credit card–related computer or computer network security. This includes providing IP addresses and network configuration diagrams for use in scanning systems for vulnerabilities.

C. Departments/units are responsible for notifying AgriLife Fiscal in the event of a suspected security breach

2.0 ESTABLISHING NEW MERCHANT ACCOUNTS

2.1 Merchant accounts must be in place before credit cards can be accepted.

2.2 Departments/units that accept credit cards must complete AG-255, *New Credit Card Merchant Application*, and submit to AgriLife Fiscal via campus mail at MS 2147.

2.3 Accounts can be revoked for failure to comply with credit card processor guidelines or agency procedures.

3.0 CREDIT CARD SECURITY

3.1 AgriLife Research and the payment card industry take safeguarding of cardholder data very seriously. Failure to comply with System, agency, and industry security regulations may result in the revocation of the department's merchant account, or in the case of lost or stolen cardholder data, assessment of severe fines on the department/unit by the bank. Departments/units are financially responsible for fines resulting from security breaches.

3.2 Before a merchant department/unit may accept credit card payments, adequate security and internal controls that meet requirements of both PCI DSS and System Regulation 29.01.03, *Electronic Information Services Access and Security*, must be developed and implemented. To provide adequate security, combined efforts of the business and information technology functions within the department are required.

3.3 The design and architecture of computer systems and networks associated with credit card processing, as well as the protocols used to transmit such data, must be approved by the AIT Network Security prior to implementation. Subsequent changes must be approved prior to implementation.

3.4 All equipment and software must comply with current PCI security standards. Non–compliant equipment or software must either be reconfigured or replaced.

3.5 Computer or computer network security and internal controls shall include, but not limited to:

A. installation and maintenance of a firewall configuration to protect cardholder data;

B. protection of stored cardholder data through encryption (Note: store as little cardholder data as necessary);

C. encrypted transmissions of cardholder data (Note: credit card data submitted via e–mail shall never be accepted);

D. the use of regularly updated antivirus software or programs;

E. development and maintenance of secure systems and applications;

F. the restriction of computer and physical access to cardholder data to authorized personnel (Note: credit card information stored on a computer must be password protected and credit card information must be encrypted. Credit card information shall be located on a drive or server with very limited access);

G. assignment of a unique user ID to each person with computer access;

H. tracking and monitoring of all access to network resources and cardholder data; and

I. regularly tested security systems and processes, in accordance with the most current best practices and PCI standards.

3.6 Business process security and internal control features shall include, but not limited to:

A. obtaining background checks for individuals authorized to have access to cardholder data, in accordance with PCI DSS items 12.7;

B. requiring that clerks conducting credit card transactions in person always keep the credit card within the customer's sight;

C. accepting credit card transactions for no more than the amount of the purchase;

D. confirming that the amount entered into the credit card machine agrees with the purchase amount;

E. assuring that the credit card expiration date is not included on the receipt;

F. ensuring that only the last 4 digits of the credit card number prints on the receipt copy given to the customer (Note: departments/units must ensure that machines meet this requirement, and must notify AgriLife Fiscal if a machine is not in compliance);

G. requiring that third–party vendors with access to sensitive cardholder data be contractually obligated to comply with PCI security standards;

H. ensuring that the storage of printed cardholder data, (such as merchant copies of receipts or daily batch reports), are secured in a location with access limited to those with legitimate business need (Note: Retain in accordance with the Systems Records retention Schedule and AgriLife Records retention procedures.);

I. requiring that the authorization of access to keys for file cabinets containing cardholder data be restricted to personnel who have a business need to such access; and

J. avoiding storage of cardholder data on portable computer devices or storage media.

3.7 In addition to the initial *PCI Compliance Questionnaire* completed during setup, AgriLife Fiscal is required to complete an annual PCI self–assessment questionnaire for each merchant account.

3.8 AIT will perform periodic reviews of computer and/or computer networks to ensure that security features are in place and are adequate to protect credit card data.

3.9 AgriLife Fiscal will periodically perform reviews of business procedures to help departments/units identify ways to better protect cardholder information.

4.0 MONTHLY SERVICE CHARGES

Monthly service charges differ for each card type. For more information on monthly service charges, please contact AgriLife Fiscal.

5.0 REFUNDS

5.1 Credit card refunds cannot be issued for more than the original transaction amount, and can only be refunded on the card used for the original purchase.

5.2 In most cases, refunds cannot be processed back to the originating card more than 180 days after the initial transaction.

5.3 In rare instances of refunds beyond 180 days, the merchant should first verify that the refund has not already been processed. If the refund has not already been processed, the merchant should submit a payment request to Accounts Payable so that a check can be issued.

6.0 DISPOSAL OF SURPLUS OR NONFUNCTIONAL EQUIPMENT

When a department/unit no longer needs a particular device to swipe or read credit cards, that card–reader must be returned to AgriLife Fiscal for disposal.

7.0 REQUIRED TRAINING

7.1 Departments/units that have access to more than one card number at a time, including information technology staff who support systems that process credit card data, are required to complete an online PCI security training course before being allowed to handle credit card information.

7.2 Upon completion of the initial PCI Security Training, employees are required to take an annual refresher course as long as they have access to more than one card number.

7.3 The department is responsible for providing sufficient training to volunteers based on the types of transactions volunteers may process.

7.4 For more information on available training, please see the AgriLife Account Receivables and E-Commerce resources Web site.

8.0 RESOURCES

Supplemental information regarding the program can be found on the AgriLife Account Receivables Web site.

DEFINITIONS

Merchant Accounts—special bank accounts issued by a merchant processing bank (also called a credit card processor) that allow a business to accept credit, debit, gift, and other payment cards

Merchant(s)—An AgriLife department/unit with a merchant account or a group of departments/units with one common merchant account are referred to as “Merchants.”

Merchant Level—classification based on transaction volume. Merchants are ranked as level 1 through 4 with Level 1 being the highest–volume merchants subject to higher security risk. Any merchant that suffers a credit card data security breach, regardless of transaction volume, is automatically elevated to Level 1.

PCI (or PCI DSS) Standards—*Payment Card Industry Data Security Standards* are created by the Payment Card Industry Security Standards Council for the purpose of safeguarding sensitive cardholder data. The precise security measures required by a department will vary depending on how credit cards are accepted—in person, over the phone, or on the internet—but all are covered in the PCI DSS.

Program Fees—monthly fees assessed based on the merchant’s total monthly net credit card sales.

RELATED STATUTES, POLICIES, OR REQUIREMENTS

System Regulation 21.01.02, *Receipt, Custody, and Deposit of Revenues*

System Regulation 29.01.03, *Electronic Information Services Access and Security*

AgriLife Research Procedure 29.01.03.A0.01, *Information Resource Procedures*

AgriLife Research Procedure 29.01.99.A0.03, *AgriLife Research Network Procedures*

Payment Card Industry Data Security Standards

AgriLife Form AG-255, *New Credit Card Merchant Application*

CONTACT OFFICE

Questions about this procedure should be referred to AgriLife Fiscal at 979-862-2245 or 979-845-0323.