UGA Cooperative Extension Service Credit Card Machine Policy

PCI compliance requires that each office have their own set of policies and procedures for handling credit cards. College wide policies reflect the minimum required policies and procedures, but each office must develop their own set of policies and procedures for compliance.

Set up Process

All offices wishing to accept credit card payments should seek and obtain approval from the district office. The set up process will be coordinated through the CAES Business Office and utilize the existing state contract. You will still be able to maintain your current banking institution; however, once approved by the district office, you must use the approved vendor and adhere to the attached procedures.

Forms of Payment

Currently Visa, Discover and MasterCard are the only credit cards that will be accepted.

Identify Credit Card Processing Terminals

All credit card processing terminals should be properly inventoried, listing department and location, with any changes communicated to your district office before relocation. The office must also verify that the terminal has retained the tamper sticker and is stored securely.

Adequately document the information for each terminal location, which is to be provided to your district office. Adequate information includes the name and phone number of the contact person, management responsible for the terminal, and other information as required by your district office and the CAES Business Office.

Securing Credit Card Processing Terminals

Secure processing terminals during and after working hours to prevent unauthorized access.

If it is possible to assign password and/or user identification to staff operating terminals this option must be utilized. This protects the integrity of the processing function by assigning passwords and/or user identification (ID), which can help prevent unauthorized use. Passwords and User Identification should not be shared.

If exception reports are available that identify violations of password and user ID usage, they are to be reviewed by the CEC.

Credit Cardholder Information
Credit Card transactions should be processed when the named card holder is present and able to present the actual card for use. Obtain accurate and valid credit cardholder information (via personal contact - cardholder present)

The credit cardholder information required to process transaction is:

- Dollar amount
- Photo ID
- Expiration date
- Signature

Use the credit card that is presented and SWIPE the card to obtain authorization and perform the transaction. (MANUAL credit card processing costs are significantly higher than SWIPE processing costs.)

**Security of Cardholder’s Information**

Credit card information should be properly secured or destroyed in a timely manner as determined by the retention schedule from the BOR Policy. Signed credit card receipts will be maintained for one year. Full credit card numbers, as well as the three digit number located on the back of the card, should never be retained for any purpose. Credit Card information or transaction reports cannot be shared, misused, or left unsecured. Violation of this policy could result in criminal prosecution.

**Processing of Credit Card Transactions**

Ensure only authorized staff process credit card transactions.

Whenever possible, process credit card transactions by SWIPPING the credit card, which is the preferred method. Credit card transactions that are processed by SWIPE cost the Center as much as 60% less than the MANUAL processing fees.

Work with your district office to obtain periodic transaction reports to assist management in determining the manner in how credit card transactions are being processed. Review them for trends by locations in processing methods (swipe vs. manual); and investigate for reasonableness of methods used and associated costs.

**Processing Credit Cards Transactions over the Phone**

Transactions accepted when the credit card is not presented pose a greater risk to the office by increasing the possibility of use by unauthorized individuals, and by compromising the office’s position in cases of disputed charges. However, if the credit cards are taken over the phone the following additional information must be recorded: full address, full credit card number (after use, all but the last 4 numbers must be punched out), full name on the card, zip code, and notation that this transaction was taken over the phone.
For additional security, have the individual eventually sign the receipt if they come to the office.

Never email anything with credit card number on it. Credit card information may be faxed if and only if the fax machine is not a multi-purpose machine.

**Processing Credit Card Refunds/Credits**

Refunds will need to be processed back to the original card only. It is illegal to refund the customer through check, cash, or other means. Since full credit card numbers are not retained, the customer would either have to bring in the card or provide the number to you for manual entry into the terminal. You must pull the original sales slip to verify the amount to ensure you do not provide a credit in excess of original purchase.

All refunds must be documented to include: the name of the person receiving the refund, the reason for the refund, the program or activity associated with the refund, the CEC signature of approval, and the customers’ signature along with a copy of the original receipt provided to the customer at the time of purchase.

**PCI Compliance Training**

UGA Cooperative Extension Services are required to complete yearly training in PCI compliance. All personnel who process credit card payments must complete this training. New employees whose job responsibilities include handling credit cards must complete PCI compliance training before handling credit cards.

Proof of training must be submitted to the district office as well as the CAES fiscal compliance coordinator.

**Daily/Monthly Processes and Reports**

County offices are required to perform the following tasks daily and procure proper authorization at all required steps:

**END OF DAY PROCESS:**

Three summary reports are available on a daily basis that provides:

1. The list of each individual card transaction that comprises the daily total (Batch Report);
2. The totals by day per card type (Batch Settlement) summary; and,
3. A summary report (Batch Report – Batch Inquiry). This report includes total dollars of sales, voids, and credits, with the quantity of each type of transaction.

At the close of each business day or at the start of the following business day, the following close out steps must be performed:
1. Print batch report.

2. Review transactions from the batch report.

3. Record transactions in daily credit card deposit record.

4. The CEC reviews and signs the daily credit card deposit record.

5. All transactions must be entered into QuickBooks Online.

Maintain the credit card transaction report for audit purposes.

The CEC’s review is to ensure all refunds/credits are supported with adequate documentation, and have been approved.

The district office should evaluate if the two additional summary reports should be reviewed to determine if they offer value as a control at the location.

MONTHLY END PROCESS:

1. Each month the following steps must be performed:

2. The daily credit card deposit record is finalized for the month.

3. The bank statement is reconciled to QuickBooks Online, the monthly credit card deposit record, and receipt book.

4. Monthly reconciliation of credit card deposit record is reviewed and approved by the CEC.

5. Monthly reconciliation of credit card deposit record is sent to the District office.

6. The CEC is responsible for contacting the district office if inappropriate credit card transactions are suspected within their office.

7. In addition, the district office analyzes credit card, monthly credit card deposit record, and bank data to help identify inappropriate transactions, and will engage appropriate office personnel as needed.

**Documentation of Credit Card Payment Process**

Each county office must document how they take and process a credit card. They must state all steps from when the credit card is received from the customer to where receipts are stored in the office.
**Other**

Terminals must be connected to an analog phone line in the office. Digital phone lines are not acceptable.

Individual office policies must include an incident response portion.

Any unique procedures or practices must be noted in individual office policies.

Only employees with a UGA background check may handle anything with credit cards.

**Questions or Comments**

Questions or comments on these guidelines can be addressed to the CAES Business Office’s Fiscal Compliance Coordinator.