GUIDELINES & APPLICATION FOR CREDIT CARD ACCEPTANCE

A department must be approved to collect funds on behalf of Kent State University before applying for credit card acceptance. The departmental management must ensure that all personnel involved in processing credit cards for their department adhere to the following guidelines.

1. Obtain approval from the Bursar's Office and, if applicable, the Office of Security and Access Management before entering into any merchant credit card agreement, acquisition, disposal, or replacement of equipment, software, internet provider or wireless device (see DEPARTMENTAL APPLICATION FOR CREDIT CARD ACCEPTANCE, page 5).

2. Comply with University administrative policy 3342-7-01.2 regarding credit card security and Payment Card Industry Data Security Standards.

3. Maintain a Employee Credit Card Processing Agreement for all personnel engaged in processing credit card transactions. The department copy should be a completed and approved by Bursar's Office personnel version.

4. Verify with Human Resources that an appropriate background check was performed, within the limits of Kent State University policy, on potential employees who will have access to systems, networks, or cardholder data.

5. Ensure that all personnel engaged in credit card transactions complete mandatory PCI-DSS security training before engaging in any aspect of credit card processing and repeat this training annually.

6. Ensure that personnel handling credit card processing, the processing of refunds, and the reconciliation function are separate individuals. If the processing of these functions cannot be separated, contact the Bursar's Office for guidance.

7. Obtain a unique user ID for each person with computer access to cardholder data. User names and passwords for all systems on which credit cards are processed may not be shared and initial default passwords must be changed by the user.

8. Immediately notify the Bursar's Office of any changes in job responsibilities or employment status that would require change to or deletion of access to credit card processing.

9. Ensure that cardholder data is never stored electronically. Written/hard copy cardholder data that is stored must be clearly marked as confidential and stored securely at all times; however, certain cardholder data may never be stored in any form including: the three or four digit CVV or CVV2 validation code from the credit card, the Personal Identification Number (PIN) or the magnetic stripe information. Methods for securing written/hard copy cardholder data may include storing in a locked drawer or locked file cabinet.

10. Written/hard copy cardholder data may only be stored until no longer needed for business or legal purposes, not to exceed 180 days. Securely destroy all written/hard copy cardholder data using a crosscut shredder or a validated record destruction service provider.

11. Restrict access to cardholder data to individuals whose jobs require such access. Establish procedures to prevent unauthorized access to cardholder data, these procedures should include, but are not limited to, the following:

    a. Hard copy containing permissible cardholder data must be stored in a locked drawer or file cabinet;
    b. Department must establish password protection on computers and credit card processing equipment;
    c. Visitor sign-in logs, escorts or other means must be used to restrict access to documents, servers, computers, and credit card processing terminals.

12. Verify that terminals, computers, and other equipment do not display or print the full 16-digit credit card number on equipment monitors or on the receipt. If any equipment or receipt is found to display the full 16-digit credit card number, notify the Bursar's Office immediately.

13. Ensure that imprint machines are never used to process credit card payments. This practice is prohibited as they display the full 16-digit credit card number on the document imprinted including the customer copy.

14. Assume complete responsibility for all cardholder data submitted for processing.
    a. Never transmit or accept cardholder data in any electronic form which would include fax or enduser messaging technology such as e-mail, instant messaging, chat, etc.
    b. Ensure that any written/hard copy card holder data received from other sources is delivered as USPS mail, secured courier, or personal delivery by individual receiving information.

15. Maintain an up-to-date list of credit card processing devices and periodically inspect device surfaces to detect tampering and/or substitution.

16. Report any breach or potential compromise of cardholder data immediately to your supervisor and to PCICompliance@kent.edu. This notice must not contain any specific cardholder information; those details will be solicited when the incident is investigated.

Credit Card Processing Instructions

Credit card transactions are monetary transactions and therefore are subject to the same control and reconciliation policies as cash and check transactions. A daily accounting of receipts should be reconciled to these electronic transactions. Credit card sales should be recorded along with any currency, coins, and checks as part of a daily deposit within CASHNet. The actual funds for credit card transactions are automatically deposited electronically into the University's bank account daily and are reconciled monthly by the Controller's Office. All fees associated with credit card transactions are charged to departmental indexes monthly for credit card terminals and quarterly for Storefronts.

Departments should follow the general instructions below to deposit and report credit card sales:

1. Credit card transactions accepted in person, by mail, and over the phone will be entered directly into the secure PCI-DSS compliant university-approved electronic application or device.

   Methods of entry include: Swiping the card into a credit card terminal; hand-keying the credit cardholder data into a credit card terminal; customer using EMV, chip and pin, slot and entering their pin number.

2. Departments using credit card terminal devices must close and settle the batch daily. Multiple batches may be completed throughout the day Using one of the two methods below, enter your deposit into CASHNet. Contact the Bursar's Office to determine what item codes to use to process your deposit to the appropriate index/fund/revenue account.
   a. Single transactions – Using the receipt from your credit card terminal
      i. Enter the Item Code(s) and amount
      ii. Enter the Payment Code and amount to correspond to your credit card transaction.
         1. CGBB = Visa and MasterCard, DSBB = Discover Card
   b. Batched transaction – Using the settlement report from the credit card terminal at the end of the day
      i. Enter the Item Code(s) and amount(s)
      ii. Enter the Payment Code(s) for your entire days deposit and corresponding amounts, may include a combination of cash, check and/or credit cards
         1. CA = Cash, CK = Check, CGBB = Visa and MasterCard totals combined, DSBB = Discover Card

3. Departments using CASHNet Storefront applications are responsible for reconciling customer payments made online to ensure revenue was recorded correctly to the general ledger in Banner Finance.

4. When a credit card dispute occurs, the department will be notified by the Controller's Office for information on the transaction in question. Charge-backs of credit card transactions will be charged to the departmental index account by the Controller's Office.

Credit Card Terminal Instructions

Once credit card processing equipment has been installed, follow the instructions below to operate your new equipment. A quick reference guide should be included the shipping package.

In order to maintain the security of your credit card terminal you must adhere to the minimum requirements.

1. Maintain a list of terminals, including the location, make, model, and serial number(s). This information will also be maintained by the Bursar's Office.
2. Regularly inspect terminal surfaces to detect tampering or replacement.
3. Train personnel to be aware of attempted tampering or replacement by:
    a. Verifying the identity of any third-party persons requesting access to the terminal.
    b. Do not install, replace, or return devices without verification from the Bursar's Office.
    c. Be aware of suspicious behavior around the terminal.
    d. Store all terminals in a locked, secure cabinet or office when not in use.
    e. Report suspicious behavior or indications of tampering or substitution to your supervisor and the Bursar's Office.

Demonstrations and troubleshooting information for Clover terminals can be found at https://help.clover.com/ .

DEPARTMENTAL APPLICATION FOR CREDIT CARD ACCEPTANCE

In order to be authorized to accept credit card payments please provide the following information:

DEPARTMENT INFORMATION

Department: _____Campus: _____

Address: _____ City _____ State _____ Zip: _____

Phone: _____ Fax: _____ Dept. Email: _____

Primary Contact: _____ Title: _____

Phone: _____ Email: _____

CREDIT CARD PROCESSING DATA

Anticipated methods of collecting payments (check all that apply):

☐ In Person ☐ By Mail ☐ By Phone

☐ Internet - With a CASHNet Storefront ☐ Internet – All other

Please list: _____

Please indicate the timeframe credit card payments will be accepted:

☐ One-time Event ☐ Annual/Seasonal Event ☐ Ongoing/Permanent

Describe the purpose for the credit card acceptance site:

_____

_____

Index / Account to which merchant, equipment, set-up and usage fees should be charged: _____

DEPARTMENT APPROVAL

I have read and agree to comply with the administrative policy 3342-7-01.2 regarding credit card processing security.

Requestor's Name: _____ Title: _____

Signature: _____ Date: _____

Email _____Phone _____

I agree that credit card acceptance is needed in this department for the purpose stated and I approve this application.

Approval Authority: _____ Title: _____

Signature: _____ Date: _____