SOUTHERN ILLINOIS UNIVERSITY EDWARDSVILLE
Bursar's Office

Cash, Payment Card, and Gift Card Handling Guidelines

OBJECTIVE: To ensure that all cash, check, and payment card collections are properly accounted for and all collections are deposited intact. To ensure the University is in compliance with Payment Card Industry Data Security Standards (PCI-DSS). To ensure that University acquired gift cards are properly handled.

NOTE: Throughout these guidelines, the term payment card is used to encompass both credit and debit card transactions.

SECTIONS:
A. General
B. Cash
C. Checks
D. Payment Cards
E. Web-Based Payments
F. Refunds
G. Reconciliation
H. Gift Cards

A. General

1. Departmental cash, check and payment card handling procedures should be in writing. See *Bursar's Office Guidance to Fiscal Officers Collection and Deposit of Cash, Checks, and Other Receipts* section of the Bursar's Office website for sample department receipt handling procedures.

2. All collections (cash, check and payment card) should be promptly recorded in department records.

3. Customers should always receive a receipt after making a payment.

4. Funds collected should be deposited daily. If minimal, funds may be held for up to one week for deposit.

5. Procedures should prohibit the disbursement of cash receipts. Petty cash funds are not permitted.

6. Adequate physical facilities, such as a safe or locked desk drawer, should be provided to safeguard cash and checks until deposited.

7. All personnel handling cash should be trained on the appropriate procedures to follow in the event of theft or attempted theft. Contact the Bursar's Office or Campus Police for more information.

B. Cash

8. In order to make change for customers, a change fund should be requested from the Bursar's Office. Department change funds should not be created by withholding receipts from a deposit. Department change funds are not to be used as a petty cash fund.

9. To ensure accountability for cash, only one person at a time should have access to a cash drawer. At the end of the day or each shift change, the cash drawer should be counted and reconciled to department records (i.e. cash register tape or daily control log).

10. It is not permitted for customers to send cash by mail.

C. Checks

11. All checks should be made payable to SIUE, not an individual or account.

12. A restrictive endorsement indicating "For Deposit Only", "SIUE", and the Budget Purpose number (e.g., 74XXX) should be stamped (or written) on each check as soon as received.

13. Post-dated checks should not be accepted. If post-dated checks are inadvertently received (such as through the mail), contact the Bursar's Office for instruction on proper handling.

D. Payment Cards

14. All payment (debit and credit) card information is confidential and should be safeguarded the same as cash.

15. No payment card information can be stored on a PC's hard drive or shared drive. It is prohibited to store the full contents of any track from the magnetic strip on a payment card whether in a secured database, log file or point-of-sale terminal. Never store the card validation code, also called the CVC2 or CVV2 number that is found on the back of the payment card.

16. Payment card information cannot be accepted by email. Payment card information can be accepted over the phone or by fax, but once the transaction is processed the full payment card number must be cross-cut shredded. If accepted by fax, the fax machine must be in a secure location and stored memory disabled so unauthorized individuals cannot access faxed documents containing payment card information.

17. Never give unauthorized personnel access to payment card information.

18. All payment card receipts must be truncated (only last four digits displayed).

Paper documents that contain full payment card numbers must be stored in a secure area and safeguarded the same as cash until such time that they can be disposed of properly by cross-cut shredding.

19. An audit list (listing of each processed transaction and a total for the batch) should be printed prior to closing the payment card terminal. Terminals should be closed out at the end of each business day.

20. Signed sales slips should be reconciled to the audit list prior to deposit.

21. Discrepancies on the audit list should be resolved with Global Payments, Inc. (1-800-916-2118 or 1-800-367-2638) the same day as the transaction and before the deposit is prepared.

22. Normally daily charge transactions exceed refund transactions. Special handling is required if refund transactions exceed charge transactions on the audit list. Contact the Bursar's Office for assistance.

23. Each department accepting payment cards is defined as a "merchant" and must designate one individual to act as the Merchant Primary Point of Contact (PPC). The Merchant PPC is responsible for:

    a. Completing the annual PCI Compliance Security Assessment Questionnaire (SAQ)
    b. Completing annual Security Awareness training and ensuring that applicable department personnel also complete training as required by the *SIU PCI DSS Information Security Policy*
    c. Documenting department procedures concerning payment cards
    d. Attending Bursar-sponsored meetings to stay abreast of Payment Card Industry Data Security Standards (PCI-DSS)
    e. Ensuring background checks have been completed prior to hiring personnel who will handle payment cards or payment card information

24. *SIU PCI DSS Information Security Policy* (under Section III, General Requirements, item G) states "each merchant must conduct a formal risk assessment annually and upon significant changes to the environment to identify threats and vulnerabilities." This requirement is met when the Merchant PPC completes the annual SAQ and the University's Qualified Security Assessor (currently Trustwave) evaluates the results. If the SAQ result is "fail" then the Merchant PPC should review their responses to make sure responses are accurate. If no corrections to SAQ are needed and result remains "fail" then contact Dawn Sparks in the Bursar's Office 650-5273 for assistance. The Bursar's Office in conjunction with ITS will work with Merchant PCC to identify operational or system changes needed to achieve a secure environment for payment card processing.

25. Physically inspect payment card terminals regularly to detect tampering with equipment. Do not allow equipment to be removed or accessed by others unless a supervisor has confirmed that equipment is to be repaired or replaced. Inspect the ID of any individual asking to repair or replace

equipment.

E. Web-Based Payments

26. The University selected CASHNet to serve as its web payment processor. University customers should enter their payment card information only on secure web sites hosted by CASHNet.

27. University-based web stores from other software vendors need to interface with CASHNet in order to accept payments on the web. If a vendor is unable to interface with CASHNet or it is cost prohibitive, an exception can be requested by contacting the Bursar's Office.

28. Do not use vendor-supplied defaults for system passwords and other security parameters.

29. All users must authenticate using, at a minimum, a unique username and password.

30. University employees must not enter customer payment card information into University-based web stores from their SIUE workstation.

31. When an employee leaves the University, that employee's user account and password must be revoked as soon as possible.

F. Refunds

32. Department policy and procedures for refunding customers should be in writing.

33. If refunds are permitted, customers should be expected to provide the original sales receipt.

34. Refunds should be made in the same manner as the original sale; if cash was paid then refund with cash; if credit card was used then refund to the same credit card.

35. Customers must sign for receipt of funds as evidence that a refund was received. Departments need to retain documentation.

36. It is recommended that a supervisor initial or approve refund transactions.

G. Reconciliation

37. To ensure receipts are properly deposited and recorded in AIS, someone other than the person(s) accepting customer payments and making the

deposit must perform the following reconciliation procedures:

a. Receipts recorded in department records equal the amount deposited at the Bursar's Office

b. Receipts recorded in department records equal the amount shown on monthly AIS Funds Available-Report of Transactions.

38. Review *Bursar's Office Guidance to Fiscal Officers Collection and Deposit of Cash, Checks, and Other Receipts* section of the Bursar's Office website for further guidance on segregation of duties and reconciliation of receipts.

H. Gift Cards

39. Gift cards should be treated like cash.

40. All unused gift cards must be stored in a secure, locked location with access restricted.

41. One person in each area should be assigned the responsibility for purchasing gift cards – the fewer the better. One back-up should also be appointed to purchase gift cards in the absence of the primary. The names of persons authorized to purchase gift cards should be provided to Purchasing.

42. Upon issuance of the cards to the ultimate recipients, the Requestor will obtain signatures of the recipients. This form will be turned in to the Gift Card Manager to be filed with the original purchase information.

43. In the event that one or more of the gift cards are not distributed, the Requestor will return them to the Gift Card Manager to be recorded on a "Return Log". These cards are available for later distribution. Unused gift cards must be kept in a locked drawer or safe.

44. The purchase of a gift card must follow all purchasing rules of the University when making any purchase from a vendor.