SOUTHERN ILLINOIS UNIVERSITY EDWARDSVILLE
Bursar's Office

Cash, Payment Card and Gift Card Handling Guidelines

OBJECTIVE: To ensure that all cash, checks and payment card receipts are properly accounted for and all receipts 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 Payment Cards
F. Proof of Receipts
G. Gift Cards

A. General

1. Cash, check and payment card handling procedures should be in writing.

2. All revenue, (cash, checks and payment card) should be promptly recorded.

3. Customers should always receive a receipt after making a payment or credit transaction.

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

5. Procedures should prohibit the disbursement of cash receipts.

6. Adequate physical facilities, such as a safe, should be provided to safeguard cash and checks until deposited. Arrangements for the transport of cash should be coordinated with the Bursar's Office.

7. All personnel handling cash should be trained on the appropriate procedures to follow in the event of theft or attempted theft.

B. Cash

8. A temporary or permanent change fund should be obtained from the Bursar's Office for cash-handling needs (such as making change). Department change funds are not to be used as "Petty Cash".

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.

11. Questions or concerns regarding discrepancies with the change fund should be coordinated with the Bursar's Office.

C. Checks

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

13. A restrictive endorsement indicating "For Deposit Only", "SIUE", and the Budget Purpose should be stamped (or written) on each check as soon as they are received.

14. 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

15. All payment card information is confidential and should be safeguarded the same as cash.

16. 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. Do not store the card validation code, also called the CVC2 or CVV2 number that is found on the back of the payment card.

17. Payment card information CANNOT be accepted by fax or email. Payment card information can be accepted over the phone, but once the transaction is processed the full payment card number must be shredded or stored encrypted on a secure server.

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

19. All payment card receipts must be truncated (only last four digits display). 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 shredding.

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

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

22. 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.

23. In instances where credits exceed charges on the audit list, contact the Bursar's Office for instructions on proper handling.

24. Each department accepting payment cards must designate an individual to act as

Merchant Primary Point of Contact (PPC). The Merchant PPC is responsible for completion of annual PCI Compliance Questionnaire, completion of annual Security Awareness training, documentation of departmental procedures concerning payment cards, training of departmental staff on safeguarding payment card information and attending Bursar sponsored meetings to stay abreast of Payment Card Industry Data Security Standards. Merchant PPC ensures that departmental personnel handling payment cards have background checks before hiring and receive annual training in accordance with the SIU PCI DSS Information Security Policy.

E. Web Based Payment Card Processing

25. The University selected CASHNet to serve as its web payment processor. Customers should only enter their payment card information on secure web sites hosted by CASHNet. University based web stores (shopping carts) need to interface with CASHNet in order to accept payment cards on the web. Existing web stores not processing through CASHNet will be expected to migrate within a reasonable period of time. All future web stores must use CASHNet e as their web payment processor.

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

27. Access to payment card account numbers must be restricted for users on a need-to-know basis.

28. All users are required to authenticate using, at a minimum, a unique username and password.

29. When an employee leaves the University, that employee's user accounts and passwords need to be revoked as soon as possible.

30. Annual PCI Compliance Questionnaire must be completed.

F. Proof of Receipts

31. Someone other than the person making the deposits should verify that all receipts were properly deposited and recorded. Collection reports should equal receipts as recorded in pre-numbered receipt books and/or cash registers. Deposits made with the Bursar's Office should be verified by agreeing the amount of each collection report to the monthly AIS Report of Transactions.

32. All refunds or adjustments should be authorized, receipted and accounted for. These duties must be assigned allowing for appropriate segregation of duties among office personnel.

G. Gift Cards

33. Gift cards should be treated like cash.

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

35. 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.

36. 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.

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

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

39. Any unused portion of a gift card must be returned to the person responsible for maintaining gift cards and their master listing. Any cash received as change after using a gift card must be deposited in the Bursar's Office to the account from which the gift card was originally purchased through a collection report. Such cash received should be treated as any cash receipt described earlier in these guidelines.