SOUTHERN ILLINOIS UNIVERSITY EDWARDSVILLE
Bursar's Office

Cash and Payment Card Handling Guidelines

Last Revised: 03.13.2026

Overview:
To ensure that all cash, check, and payment card (both credit and debit card) collections are properly accounted for and all collections are deposited intact. To ensure the University is compliant with Payment Card Industry Data Security Standards (PCI-DSS).

General:
- Departmental cash, check and payment card handling procedures should be in writing.
- All collections should be promptly recorded in department records.
- A receipt for each transaction should be made available to the customer, either paper or email.
- Funds collected should be deposited daily. If minimal, funds may be held for up to one week for deposit.
- Procedures should prohibit the disbursement of cash receipts. Petty cash funds are not permitted.
- Adequate physical facilities, such as a safe or locked desk drawer, should be provided to safeguard cash and checks until deposited.
- All personnel handling cash should be trained on appropriate procedures to follow in the event of theft or attempted theft. Contact the Bursar's Office or Campus Police for more information.

Cash:
- In order to make change for customers, a department change fund should be requested from the Bursar's Office. Department change funds are not to be used as petty cash funds.
- To ensure accountability for cash, only one person at a time should have access to a cash drawer. At the end of the day/shift change, the cash drawer should be counted and reconciled to department records (i.e. cash register tape, POS activity report, or daily control log.
- Due to the discontinuation of pennies by the Federal Government, State and/or Federal guidance is expected to be issued in the near future. Until such guidance is adopted, symmetrical rounding is permitted when applied automatically through register or software programming.

    - In situations where automated rounding is not available, departments are encouraged to provide exact change when possible. If exact change cannot be provided, departments may either apply symmetrical rounding or round down to the nearest nickel, provided an over/short reconciliation process has been established to account for rounding differences.
    - The rounding-down option is considered acceptable as an interim measure to help avoid potential customer confrontations pending adoption of a state or national standard.
- Customers should be discouraged from sending cash by mail.

Checks:

- All checks should be made payable to SIUE, not an individual or account. In order for the checks to be adequately scanned to the bank, please encourage customers to write checks in either black or blue ink.
- A restrictive endorsement indicating “For Deposit Only”, “SIUE”, and the Budget Purpose number (e.g., 74XXXX) should be stamped (or written) on the back of each check as soon as received.
- 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.

Payment Cards:

- All payment (debit and credit) card information is confidential and should be safeguarded the same as cash.
- 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.
- Payment card information cannot be accepted by email. It is not recommended to accept payment card information over the phone or by fax, especially in cases where a TEAMS phone is being used.
    - If payment information IS taken over the phone, it is recommended to enter the transaction directly into the credit card terminal.
    - In cases where the information is written down, once entered into the credit card terminal, the document must be cross-cut shredded.
    - If payment information is 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.
- If a refund is required to be processed on a payment card, the card must be present and a supervisor must authorize. In cases where the card is not present, a request

can be sent to the Bursar Office to refund all or part of the transaction in the State of Illinois ePay portal.

- Never give unauthorized personnel access to payment card information.
- All payment card receipts must be truncated to display no more than the first 6 and last 4 digits of the card number. Paper documents that contain the full payment card numbers must be stored in a secured area and safeguarded the same as cash until such time as they can be disposed of properly by cross-cut shredding.
- 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, either manually or by auto settlement.
- Signed sales slips should be reconciled to the audit list.
- Totals will be posted the departments budget purpose by Administrative Accounting upon receipt into the bank account.
- 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:
    - Inspecting machines monthly for evidence of tampering and keeping inspection records.
    - Completing the annual Security Awareness training and ensuring that applicable department personnel also complete training as required by the *SIU PCI DSS Information Security Policy*.
    - Documenting department procedures concerning payment cards.
    - Ensuring background checks have been completed prior to hiring personnel who will handle payment cards or payment card information.
- 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 University completes the annual SAQ and the University's Qualified Security Assessor (currently CampusGuard) evaluates the results.
- 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.

Web-Based Payments:

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

- University-based web stores from other software vendors are encouraged to interface with Nelnet to accept payments on the web. If a vendor is unable to interface with Nelnet or it is cost prohibitive, an exception can be requested by contacting the Bursar's Office.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- All users must authenticate using, at a minimum, a unique username and password.
- University employees must not enter customer payment card information into University-based web stores from their SIUE workstations.
- When an employee leaves the University, that employee's user account and password must be revoked as soon as possible.

Refunds

- Department policy and procedures for refunding customers should be in writing.
- If refunds are permitted, customers should be expected to provide the original sales receipt.
- 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 (see instructions under "Payment Cards").
- Customers must sign for receipt of funds as evidence that a refund was received. Departments need to retain documentation.
- It is recommended that a supervisor initial or approve refund transactions.

Reconciliation

- 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:
    - Receipts recorded in department records equal the amount deposited at the Bursar's Office.
    - Receipts recorded in department records equal the amount shown on monthly AIS Funds Available-Report of Transactions.
- Review *Bursar's Office Guidance to Fiscal Officer* resource on the Bursar 's Office website for further guidance on segregation of duties and reconciliation of receipts.