Table of Contents

I. Treasury Operations Overview

A. Purpose

To establish University policies and procedures for:

- accepting, depositing, recording, safeguarding, and reconciling all cash assets (i.e., U.S. coin and currency, checks drawn on U.S. banks and issued in U.S. dollar values, ACH credit transactions, credit card sales drafts, wire transfers, and currency and checks in foreign funds);
- managing personnel issues related to cash handling;
- entering into banking relationships on behalf of the University; and,
- processing credit card transactions and complying with Payment Card Industry Data Security Standards (PCI DSS).

B. Policy

Each cash handling unit of the University is to institute controls and procedures to ensure the physical security of cash, maximize the use of cash funds, and accurately record the receipt of cash to ensure the reliability of financial data. Units must conduct all treasury operations in conformity with E-1-3 Fiscal Roles and Responsibilities, E-1-4 Internal Control, E-17-6 Reconciliation and Review of Financial Transaction, and the provisions of this Treasury Operations Manual.

Exceptions to treasury operations policies and procedures will be considered only upon submission of an exception request as outlined in E-1-2 Requests for Exceptions to Business Procedures. Only University Financial Services may approve such requests.

Additional policies are contained within each section of this manual.

C. Responsibilities

Also see E-1-3 Fiscal Roles and Responsibilities.

1. Executive and administrative officers, including the President, Provost, executive vice presidents, Controller, associate and assistant vice presidents, associate and assistant provosts, deans, and directors must ensure that treasury operations over which they have control are operating in accordance with the policies set forth in this manual.
2. University Financial Services
    a. Treasurer
        1) Establish and enforce policies and procedures governing the receipt, handling, custody, investment and disbursement of funds;
        2) Establish and maintain records giving full account of monies received and paid by the University;
        3) Establish all banking depositories used for University funds;
        4) Establish and terminate imprest cash funds and set limits on the amount and use of such funds;
        5) Establish and enforce minimum security standards applicable to all University cash handling operations;
        6) Request, as deemed necessary, audits of any aspect of the cash receiving and handling functions of the University; and
        7) Establish procedures for accepting credit card payments and coordinate the campus wide program to ensure compliance with the Payment Card Industry Data Security Standards (PCI DSS).

b. Treasury Services
   1) Serve as the central collection point for University funds;
   2) Establish procedures and internal controls for processing and depositing cash receipts;
   3) Manage University transactional banking processes;
   4) Coordinate electronic banking transactions in accordance with applicable banking standards;
   5) In conjunction with Human Resources Training and Development (HRTD), conduct cash handling classes to ensure personnel are adequately trained on University policies and procedures;
   6) Assist organizational units in their cash handling practices;
   7) Monitor account balances and transfer funds as needed between bank accounts to ensure liquidity and proper and efficient use of funds;
   8) Maintain deposit records;
   9) Manage imprest accounts
      a) Review and approve requests for imprest funds;
      b) Review and approve imprest bank accounts;
      c) Recall an imprest fund when it is in the best interest of the University to do so.

c. Merchant Card Services
   1) Review proposed credit card transactions process and coordinate the setup of credit card processing for organizational units;
   2) Administer the credit card processes of University departments;
   3) Manage the University merchant card banking processes;
   4) Coordinate the PCI DSS compliance program and administer the Self-Assessment Questionnaire process.

d. Research Financial Services (RFS)
   Post all grant and contract related deposits and corrections to receipts. Treasury Services will notify SPA daily of grant and contract related deposits that have been received in Treasury Services.

e. Accounting and Financial Reporting Services (AFRS)
   1) Reconcile bank and state cash accounts;
   2) Initiate transfer of funds between local and state accounts for daily disbursement of funds.

3. Organizational units (e.g., administrative area, college, department, division, center, or office):

a. Department Head
   1) Establish internal controls within the department in accordance with E-1-4 Internal Control
      a) Separation of duties
         1. Perform the cash handling functions of accepting cash, voiding transactions, balancing cash, preparing deposits, recording transactions, and reconciling accounts so that no single person has control over the entire process;
         2. The following should be considered when separating cash handling duties:
            a. accepting cash and performing voids
            b. accepting cash and balancing cash daily
            c. accepting cash and preparing deposit
            d. performing voids and balancing cash daily

e. balancing cash daily and preparing deposit
f. preparing deposit and reconciling accounts

3. If staffing levels do not permit this separation of duties, identify and establish compensating controls or other controls to properly perform this function;
4. In all cases, someone other than the person receiving the funds must review and approve cash transactions daily or as transaction frequency dictates.

b) Security
1. Limit access to cash and keep funds secure at all times in accordance with Section IV, Security;
2. Ensure that security guards, local or campus police, or an armored car service is used to transport cash when circumstances require;
3. Ensure all credit card information is received and maintained in a secure manner in accordance with the Payment Card Industry Data Security Standards (PCI DSS).

2) Ensure that employees hired in cash handling positions meet the requirements listed in Section VI, Personnel Related Issues and are instructed precisely as to their duties and responsibilities;
3) Supervise all cash activities so that all funds received are properly recorded, deposited, and reconciled in accordance with University policy and procedures;
4) Establish additional cash handling policies and procedures specific to the unit's needs;
5) Conduct periodic reviews of cash activities, including reconciliations, to determine that all systems are functioning as intended and that all applicable University policies and procedures are being followed;
6) Approve all imprest cash fund requests and ensure that persons responsible for imprest cash funds reconcile the accounts on a monthly basis per guidelines in Section III, Imprest Funds;
7) Approve credit card processing applications and ensure that the credit card processes are in compliance with the applicable procedures in Section IV, Security and Section VIII, Credit Card Processing.

b. Individual employees responsible for handling cash and reconciliations
1) Receive funds and deposit them in accordance with this manual and other University and departmental policies and procedures;
2) Maintain proper records and make entries promptly and accurately;
3) Collect returned checks originally received by the organizational unit;
4) Reconciliations (Also see E-1-3 Fiscal Roles and Responsibilities and E-17-6 Reconciliation and Review of Financial Transactions)
a) Verify that the unit receives credit for all deposits and that the proper accounts are credited.
b) Persons responsible for any accounts receivable, clearing account, deferred income and refundable deposits must reconcile the balance of the detail to the balance shown on

the general ledger monthly. These reconciliations must be available for the Office of the Treasurer or Internal Audit as requested.

c) Persons responsible for imprest funds must reconcile funds per instructions in Section III.C.2.e.

d) Persons responsible for credit card payments must reconcile credit card payments posted to general ledger to the statements provided by the credit card processor.

5) Report violations of policies and procedures as required by E-1-4 Internal Control Section IV.F.

4. Imprest cash fund custodian
   a. Accept personal liability for cash losses and discrepancies in the imprest fund;
   b. Manage the imprest fund in accordance with Section III, Imprest Funds.
5. Merchant department
   a. Any department accepting credit card payments on behalf of the University for gifts, goods or services (the "merchant department") must designate an individual within that department who will have primary authority and responsibility for credit card transaction processing. This individual is referred to as the Merchant Department Responsible Person or "MDRP".
   b. The MDRP must:
      1) Execute on behalf of the merchant department the process to implement acceptance of credit card payments described in Credit Card Transactions Section VIII.B.1.
      2) Ensure that all credit card data collected by the merchant department while performing University business, regardless of how the payment card data is stored, is secured.[1]
   c. The department must annually submit to Merchant Card Services a completed PCI DSS Self-Assessment Questionnaire (SAQ.)

D. Definitions

- *Automated Clearing House (ACH):* A nationwide electronic funds transfer (EFT) system that provides for inter-bank transfers of funds. The ACH is a secure, private electronic payment transfer system that connects U.S.

[1] Data is considered to be secure only if the following criteria are met:
- Only those with a need-to-know will be granted access to credit card payment data.
- E-mail must not be used to transmit credit card or personal payment information.
- Credit card or personal payment information must never be downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.
- The three digit card validation code (CVV2, CVC2) printed on the signature panel of a credit card must never be stored in any form.
- If it is necessary to display credit card data, all digits except the last four digits of any credit card account number must always be masked.
- If it is necessary to maintain physical records, documents containing credit card and/or personal payment data must be securely stored in a locked file cabinet.
- All physical and electronic credit card and personal payment data that is no longer deemed necessary or appropriate to store must be destroyed or rendered unreadable.

financial institutions. ACH transfers typically take one to two days to complete and are the most cost effective form of electronic funds transfer.

- *Cash:* U.S. coin and currency
- *Cash Equivalent:* Checks drawn on U.S. banks and issued in U.S. dollar values, ACH credit transactions, credit card sales drafts, wire transfers and foreign funds (currency or check)
- *Cash Receipt Form:* A written acknowledgment for each cash payment received
- *Cash Receiving Location:* An organizational unit that collects cash on behalf of the University
- *Change Fund:* A type of imprest fund used only for making change for cash sales and authorized only for units handling currency and coin sales.
- *Credit Card*: A card issued by a financial company giving the holder an option to borrow funds at a point of sale; also called "Payment Cards" or "Merchant Cards"
- *Credit Card Processor*: A credit card processor, also known as an "acquirer", contracts with merchants to enable the processing of credit card transactions. The card processor authorizes each credit card transaction for the merchant, collects the funds for those transactions from the cardholders issuing bank, and deposits the total amount of each settlement batch into the university's bank account.
- *Custodian:* A full-time University employee responsible for an imprest fund's safekeeping and proper usage
- *Direct Deposit:* Transfers made from an organization's account to the accounts of employees, shareholders, vendors and trading partners using ACH
- *Foreign Funds:* Currency issued by a non-U.S. government and checks written on non-U.S. banks or for non-U.S. dollar values.
- *Imprest Fund:* An advance from the University to an individual custodian to provide change or make payments of relatively small amounts for authorized purchases of supplies, non-personal services and research subjects
- *Lockbox:* A service offered by banks where the bank receives, processes, and deposits payments and provides detailed information relating to the deposits to University organizational units
- *Merchant*: Any unit that accepts credit card payments
- *Merchant Card:* Another name for a credit card
- *Overage or Shortage:* Discrepancy between total receipts per cash receipt forms or register totals and actual amount of cash deposited. Record on the cash transmittal per instructions in Section II.B.2.g.
- *Payment Application Data Security Standard (PA-DSS):* A standard applied to any software application or system that processes credit card payments. PA-DSS payment applications do not store secure data including magnetic stripe, CVV2, or PIN, and are compliant with the Payment Card Industry Data Security Standards (PCI DSS).
- *Payment Card*: Another name for a credit card
- *Payment Card Industry Data Security Standards (PCI DSS):* A set of guidelines, measures, and controls developed to help merchants who process credit card transactions implement strong security precautions to ensure safe credit card usage and secure information storage
- *Petty Cash Fund:* Another name for an imprest fund

- *Payment Request Document (PRD):* Electronic document used for certain payments to vendors.
- *Point of Sale System:* An electronic cash register or an integrated computer system, a cash drawer, a credit card reader, and a receipt printer that records the business transaction for the sale of goods or services
- *Principal Investigator (PI):* The University's full-time faculty or staff member listed on the award notice from a sponsoring agency
- *Returned Check:* A check issued to the University of Kentucky (or affiliated organization) and refused payment by the bank upon which it was drawn
- *Safekeeping Device:* A fire-resistant storage container (e.g., safe, chest, cabinet, desk, or lockbox) equipped with at least one locking device. Safes purchased after April 1, 2013, are required to have dual locking devices such as two keys or a key and combination to obtain entry.
- *Transmittal Form:* A form accompanying a deposit of funds documenting the transmission of the funds from a cash receiving location to either Treasury Services or the bank. To access the online Cash Transmittal system sign onto myUK (https://myuk.uky.edu/irj/portal), and then follow the three steps listed below:
    1. Click on the Enterprise Services tab
    2. Click on Financials
    3. Click on the Cash Transmittal link
- *Wire Transfer:* A method of electronic transfer of funds from one bank to another bank. The Federal Reserve Wire Network typically processes domestic wire transfers and the Society for Worldwide Interbank Telecommunications (SWIFT) typically handles international wire transfers. Domestic wires take place within one day while international wires may take five days or longer.

E. **Procedures**

See each section of the Treasury Operations Manual for procedures related to that function.

II. Receipts and Deposits

A. Policy

1. Sales

   Make all sales on a cash basis unless approval to extend credit has been granted by the Area Fiscal Officer and the Office of the Treasurer has been notified.
2. Deposits
   a. For organizational units in Lexington, deposit cash directly with Treasury Services, by an armored car pickup arranged and approved by Treasury Services, or by a lockbox operation established by Treasury Services.
   b. For organizational units outside Lexington, make deposits to the authorized depository bank.
   c. Cash deposits
      1) Deposit all cash intact. No checks may be cashed or disbursements made, including reimbursement of petty cash expenditures, from receipts.
      2) Do not send cash by campus or U. S. mail.

d. Check deposits
   1) Accept checks only for amounts owed to the University of Kentucky.
   2) Checks must be payable to the University of Kentucky or appropriate affiliated organization unless checks are for deposit to an agency account. Checks for deposit to agency accounts must be made payable to the organization. See BPM E-17-14 Agency Cost Center Policies and Procedures for more information regarding agency accounts.
   3) Checks presented must meet the following requirements:
      a) Date must be current;
      b) Presenter must sign or endorse;
      c) Numeric and written amounts must agree;
      d) Be legible and in ink (if written);
      e) Not be altered or grossly mutilated;
      f) Not have any unreasonable restrictions placed on the face that limit application;
      g) Contain sufficient information to permit tracing the presenter (e.g., name, current address, or telephone number); and
      h) For checks presented in person in payment for goods and services (not gifts), some form of photo identification (e.g., state, federal or UK employee or student ID), should be checked to verify the identity of the presenter.

e. ACH and wire transfers
   Due to the significant cost savings, the University's preferred method of electronic funds transfer is ACH. Treasury Services will process all electronic funds transfers via ACH unless there is a compelling reason that the payment must be delivered on the day of the transfer request. Treasury Services will charge the initiating department for bank wire fees.

f. Credit cards
   All organizational units that elect to receive credit card payments must be preapproved as an authorized merchant department in conformance with Section VIII, Credit Card Payments.

g. Gifts
   College, program, or Office of Development gift officers must forward gift receipts on separate transmittals (not co-mingled with other types of deposits) within 24 hours to the Office of Development for processing and donor acknowledgement in accordance with E-22 Policies and Procedures for Soliciting, Receiving, Recording and Acknowledging Gifts.

h. Grants and contracts
   Research Financial Services (RFS) processes all payments for grants and contracts. Forward receipts on separate transmittals to SPA within 24 hours.

i. Reduction of expenses
   Certain payments received by the University are not revenue and must be recorded as a reduction of the related business expense (i.e., vendor refunds or rebates). Any transmittal with a credit to an expenditure G/L account (5XXXXX) must have a copy of the original source document used to pay the expense (e.g., vendor invoice, DAV,

PRD, or purchase order) attached. Treasury Services will deposit receipts without proper documentation attached to a general department or college income account.

3. Refunds
   a. Refunds for merchandise are permitted only upon presentation of the receipt issued at the time of sale.
   b. Refunds are permitted only for merchandise returns and for return of small cash deposits (e.g., key, breakage, library, or locker deposits).
   c. Process credit card refunds only via a credit card refund draft according to procedures provided by the merchant card processor. As noted in Section VIII, it is not permitted to give refunds by cash or check for purchases made by credit card.
   d. Process all other refunds by PRD, charging the cost object and G/L account originally credited.
4. Returned checks - Organizational units must undertake a continuing and diligent effort to track, physically control, and collect unpaid checks.

B. Procedures

1. Receipt Forms
   a. Create a receipt form for all sales and give the payer a copy of the receipt.
      1) Acceptable receipt forms include:
         a) Computerized point of sale system printed receipts; and
         b) Preprinted and pre-numbered receipt forms that can be completed manually.
      2) Receipt forms must include:
         a) The amount of the payment;
         b) The mode of payment (e.g., cash or check);
         c) Name of person making payment;
         d) Purpose of payment;
         e) Date of payment;
         f) Sequential number;
         g) Account payment applied to, if applicable; and
         h) Initials of the employee receiving funds for written receipts.
   b. Count cash drawers and balance to the totals of the cash receipts at the end of each shift. Report any difference in the total of the actual receipts and the total of the receipt forms as a shortage or overage on the transmittal form.
   c. Two employees must not work out of the same cash drawer.
   d. Keep records of cash receipts, voided forms, and daily transactions, substantiated by receipt forms and copies of transmittal forms. Maintain these records for three years per the University Records Retention Policy.
2. Cash and check deposits
   a. Deposit slips
      1) Order pre-printed department specific deposit slips from Treasury Services to be delivered to the department. These deposit slips have three copies (white, pink, and yellow).
      2) Prepare a separate deposit slip for each transmittal. Deposit cash and checks on separate deposit slips and transmittals. Cash or checks may be summarized on the deposit slip.

3) Place the white deposit slip with the funds to be deposited in the tamper resistant plastic bag;
4) Attach the yellow copy of the deposit slip to the T.S. copy transmittal form; and
5) Attach the pink copy of the deposit slip to the department copy transmittal form

b. Cash and check transmittal forms
1) Submit to Treasury Services a completed Cash Transmittal Form for all cash deposits (see II.B.2.c. below) or a completed Check Transmittal Form for all check deposits (see II.B.2.d.)
2) Include a unique transmittal number on the form, fill it in completely, and list each different cost object (e.g., WBS element, cost center, fund or internal order).
3) List each check separately on the Check Transmittal Form. While there is no limit for how many checks can be entered on a Check Transmittal, the online system times out after 60 minutes. For deposits involving large numbers of checks, it is recommended to divide the deposit and create 2 or more deposits to avoid the timeout limitation. Maintain a copy of the transmittal form in the unit.
4) Cash and checks for gifts, grants and contracts must be on a separate transmittal than deposits for other cost objects unless a single check is split between different types of cost objects.
5) Deliver the original and a copy of each transmittal to Treasury Services with the deposit. Treasury Services will stamp each with the date and time, and the clerk will initial as a receipt of delivery. The department will receive the copy and Treasury Services will retain the original.

c. Cash deposits
1) Prepare cash deposits as follows:
a) Currency facing the same way
b) Sorted by denomination
c) Banded ($1 bills in $100 bundles and other denominations in $500 bundles) and bands stamped with department number or name. Bands, wrappers, and coin envelopes are available from Treasury Services.
d) Coins in rolls and unrolled coins in a coin envelope
2) Place deposits in sealed tamper resistant bags obtain in Treasury Services, labeled with the following information:
a) Person preparing deposit
b) Document number
c) Department five-digit number;
d) Amount of deposit listed on the "Cash" line;
e) Date of deposit

d. Prepare check deposits as follows:
1) Restrictively endorse checks immediately upon receipt as follows:

For Deposit Only
University of Kentucky
Department Name Department Number
Restricted Trust Account Number

The endorsement may be applied by a stamp or written on each check. Units in Lexington may obtain restrictive endorsement stamps from Treasury Services. Units outside of Lexington should contact their local depository bank or approved office supply vendor.

2) Include the details of all checks, including the maker, date received and amount on the check transmittal.
3) Prepare check deposit packages as follows:
   a) Endorsed checks facing the same way;
   b) Adding machine tape in the same sequence as the checks.
4) Place deposits in sealed tamper resistant bags obtain in Treasury Services, labeled with the following information:
   a) Person preparing deposit
   b) Document number
   c) Department five-digit number;
   d) Amount of deposit in listed on the "Checks" line;
   e) Date of deposit

e. Make all deposits as follows:
   1) daily, if cash receipts accumulate to $500, although more than one deposit a day is not required;
   2) each time during the week deposits accumulate to $500 if receipts are less than $500 per day;
   3) on the last working day of the week if cash is on hand; or
   4) by 2:30 pm (Treasury Services on campus) or the local bank's cut off time (out-of-town locations) on the last working day of the month if cash is on hand in order to ensure that activity is included in the correct accounting period.

f. Departments must use their copy of the transmittal form as source documentation to verify the amount deposited and recorded in SAP when reconciling the transaction on the monthly ledger as required by E-1-3 Fiscal Roles and Responsibilities, E-1-4 Internal Control, and E-17-6 Reconciliation and Review of Financial Transactions.

g. Overages and shortages must be reported and explained on the transmittal form and must be initialed by the unit administrator. Record them by using the department's income cost center with the G/L account 449060. For shortages of $100 or more, see the additional reporting requirements in Section VII Reporting Losses.

3. Lockbox receipts and deposits
   a. Organizational units with cash receipts processed by lockbox will provide Treasury Services with the appropriate account information for crediting deposits.
   b. Treasury Services will post lockbox receipts for all cost objects except grants and Student Account Services daily based on reports from the lockbox provider bank.
   c. Sponsored Projects Accounting will post lockbox receipts for grants and contracts.
   d. Student Account Services will post lockbox receipts for their specified lockbox.
   e. The lockbox provider bank will forward deposit slips and copies or images of all checks, envelopes, and correspondence to the respective

department unless the organizational unit elects to receive copies of documents electronically.

4. ACH and wire transfer receipts and deposits
   a. Submit to Treasury Services a completed ACH Transmittal Form for all ACH deposits or a completed Wire Transmittal Form for all wire transfer deposits.
   b. Organizational units expecting funds by ACH or wire transfer must send the following information to Treasury Services on the appropriate transmittal form:
      1) Date the ACH or wire transfer is expected;
      2) Amount expected;
      3) Source (e.g., agency, company name, or person's name); and
      4) The cost object and GL to which the payment will be credited.
   c. Treasury Services maintains a list of ACH and wires for which there is no transmittal form. Organizational units that have not received credit for an ACH or wire they expected to receive should contact Treasury Services to request a copy of the unclaimed ACH and wire list.
5. Out-of-town deposits
   Prepare "Out of Town Bank" Transmittal Forms on the online Cash Transmittal system for locations outside of Lexington (i.e., 4-H Camps and Agricultural Substations) as follows:
   a. Cash and checks can be combined on the same deposit.
   b. Prepare a deposit slip for the total of cash receipts in triplicate.
   c. Deposit cash in the authorized bank in the community in which the unit is located.
   d. Record each deposit on a separate transmittal with the corresponding deposit slip attached. Transmittals must be scanned and emailed or faxed to Treasury Services within 24 hours of the deposit. For questions and complete instructions for Out-of-Town locations, contact Treasury Services at (859) 257-1983. Fax number is (859) 323-9911.
   e. To the extent feasible, an individual other than the cashier or bookkeeper must prepare transmittals and bank deposit slips. If this is not practical, the supervisor or department head must review the reconciliation of cash receipts transactions to the transmittal and deposit slip daily.
6. Foreign funds
   a. Immediately forward all foreign funds to Treasury Services using a separate transmittal form with the amount column left blank. Treasury Services will submit the funds to a depository bank for exchange. When exchanged funds are received from the bank, Treasury Services will record the appropriate amount on the transmittal form and send a copy of the form to the responsible department.
   b. For assistance in determining if a check is foreign, call Treasury Services at (859) 257-1983.
7. Deposit corrections
   a. Deposit corrections are made when there is a discrepancy between the amount of cash or checks in the deposit package and the amount listed on the deposit slip and transmittal.
   b. If the bank notifies Treasury Services of a deposit discrepancy, Treasury Services will notify the department representative who signed the transmittal. A deposit correction will be made to the general ledger

account, cost object, and fund used for the original deposit unless multiple accounts and funds were credited on the transmittal form. In this case, Treasury Services will consult with the department representative to determine the appropriate corrections.

c. If there is a discrepancy between the amount listed on the transmittal form, the amount listed on a deposit package and the amount of the deposit slip delivered to Treasury Services, Treasury Services will correct the deposit prior to delivery to the bank. Treasury Services will report the discrepancy to the signer on the transmittal.

d. Deposit corrections can also result from bank error. In this case Treasury Services will investigate discrepancies and make correcting entries as appropriate.

e. Treasury Services will adjust lockbox deposits using the above outlined procedures.

f. Final resolution of the discrepancy and adjustment of the appropriate accounts lies with the manager of Treasury Services. For discrepancies that result in shortages of $100 or more, the manager of Treasury Services will perform the additional reporting requirements in Section VII Reporting Losses.

8. Unclaimed receipts

Treasury Services will transfer any deposits unclaimed for 60 days to a general University revenue account.

9. Returned checks

a. Recording returned checks

1) University depository banks will redeposit checks returned for insufficient funds a second time.

2) Checks deposited to the Lexington bank that remain unpaid after the second presentment will be returned to Treasury Services.

3) Treasury Services or Sponsored Projects Accounting, depending upon the cost object, will prepare debit (negative) cash receipt entries for all returned checks, reducing the original account credited by the deposit.

4) A notice and the unpaid check will be sent to the organizational unit that made the deposit.

b. Collection efforts

1) When the maker of the returned check is a student, the organizational unit will send the student a letter containing the following information:

a) Notice that the check has been returned;

b) The reason the check was returned;

c) The date the check was returned;

d) That a service charge has been assessed;

e) The total amount due the University;

f) That payment is due immediately;

g) That if the check is not paid, the student will be reported to the Registrar's Office as delinquent and all transcripts will be withheld; and

h) That the student will not be able to register for future semesters until the delinquency is satisfied.

2) When the maker of the returned check is not a student, the organizational unit should send a letter containing the following information:
   a) Notice that the check has been returned;
   b) The reason the check was returned;
   c) The date the check was returned;
   d) That a service charge has been assessed;
   e) The total amount due the University;
   f) That payment is due immediately; and
   g) That if not paid within 21 calendar days, the organizational unit will send a second letter to the external party indicating that future collection efforts will be made by a collection agency.
3) For returned checks on grants and contracts other than clinical trials, the organizational unit should contact SPA concerning collection issues related to the project's invoice.
4) If the collection efforts outlined above are unsuccessful, contact Treasury Services to submit the checks to a collection agency.

c. Payment of returned checks
When the maker pays the returned check, the department will include the payment on its daily transmittal form with its other checks.

III. Imprest Funds

A. Policy

1. Permissible disbursements
   a. In accordance with the Kentucky Revised Statute 164A.560, no disbursements are to be made from imprest funds except to satisfy a liability of the University that was incurred for authorized purposes.
   b. A custodian is authorized to make small cash disbursements from the fund only for the specific purpose for which the fund was established (e.g., custodians may not use imprest funds to pay for expenditures if the fund was established for making change).
2. Imprest bank accounts
Custodians of imprest funds are encouraged to protect such funds by maintaining them in a bank account at the University's approved depository financial institution.
3. Commingling of funds
Do not commingle imprest funds with other University or personal funds.
4. Custodians
   a. Payment to research subjects
   Only the PI of a sponsored project is eligible to serve as custodian of an imprest cash fund that will be used to compensate research participants.
      1) A PI may choose to delegate signature authority or transfer funds to a subordinate within the same department for operations consistent with the authorized use and purpose of the fund. However, the PI remains personally responsible for the funds.
      2) Repayment of imprest funds is due no later than 15 calendar days after study completion or project end date, whichever occurs sooner.

3) All payments to research subjects must be made on or before the project end date to be considered allowable costs.

b. Imprest funds other than for payment to research subjects
The custodian must be an employee of the University and must be approved by the department head.

B. Types of imprest funds

1. Change funds
Change funds are authorized for units with cash handling functions and may be issued on a permanent basis or for a one-time event such as a fund-raising activity. The custodian is responsible for these funds until the advance is repaid to the University or until they properly transfer the fund to another approved custodian.
2. Small purchase/expenditure funds
Expenditures made from an imprest fund must follow the University purchasing regulations. Custodians responsible for this type of imprest fund must be thoroughly familiar with State purchasing rules and regulations to ensure that disbursements are allowable.
3. Overseas expenditures
   a. A principal investigator (i.e., University faculty or staff member) may obtain a grant that entails working in a foreign country where U.S. currency or checks cannot be used. In these instances, a temporary advance is made to the PI for expenditures, other than travel, necessary to carry on the work of the grant.
   b. All travel expenses must be kept separate and reimbursed as outlined in E-5-1 Reimbursement of Travel Expenses.
4. Payments to research subjects
University research projects sometimes require the participation of human subjects, and in order to accomplish the goals of the project, payment is offered as an incentive to encourage participation. Payments from an imprest fund for this purpose are limited to $500 or less and must be authorized by the PI. Also see E-9 Compensation to Research Subjects.
5. Travel advances
See E-5-2 Travel Advances and Repayments.

C. Procedures

NOTE: Prior to establishing an imprest fund the custodian's department should verify that a Declining Balance Procurement Card cannot meet the needs of the imprest fund requestor (see E-7-16 and E-9).

1. Establishing an imprest fund
   a. To establish an imprest fund a custodian's department must complete the Imprest Request Form and attach electronically to a PRD containing the following information:
      1) Amount requested;
      2) GL account 139000 (accounts receivable for employee advances);
      3) Fund 0021700800;
      4) Department head signature/approval;
      5) Indicate the type of fund requested; and
      6) For a temporary fund, the date the imprest account will be closed.
   b. Imprest bank accounts

1) If a bank account is needed for the imprest fund, submit a letter to Treasury Services from the custodian and the department Business Officer requesting the account. The letter must also include a list of authorized signers for the account.
2) If approved, the bank account must be in the name of the custodian **and** the University of Kentucky, and include the department or organization name and campus address.

c. The amount requested must be justified by a detailed budget and is limited to an amount that is reasonable to carry out the essential activities for which the fund is authorized.
1) For change funds, expenditure funds, and funds established for payments to research subjects, the requested amount should not exceed 45 calendar days of estimated expenses.
2) For overseas expenditure funds, the amount requested may be sufficient to cover the term of the overseas project. If the funds are required in a foreign currency, the custodian is responsible for the conversion of the advance and any unspent monies back into U.S. currency.

2. Maintaining an imprest fund
a. The custodian must keep paper or electronic copies of all PRDs and supporting documentation.
b. The custodian must maintain detailed records (e.g., name, address, payment dates and amounts) for audit purposes that specifically support the payments and maintain these records for three years after the end of the audit per the University Records Retention Policy.
c. Change orders
1) Custodians may request the ability to exchange cash for different denominations directly through the University's financial institution.
2) The financial institution will provide an Access Code and PIN number for use by the custodian for submitting currency and coin orders through an automated telephone dial-in ordering process. The automated system is a computerized voice response system that allows the custodian to order currency and coin 24 hours a day. The system will provide a confirmation and custodians may place orders up to one week in advance.
a) Before placing a change order through the automated system, the custodian must verify that the bank account balance tied to their imprest fund is sufficient to avoid any overdraft fees or delay in processing the request.
b) The cut-off time for ordering cash is 10:30am. Orders placed before 10:30 am will be delivered to Treasury Services or to the units serviced by the University's armored car provider on the next business day.

d. Reimbursements (also called replenishments)
1) Reimbursements must occur regularly (at least monthly) and in accordance with University fiscal year-end procedures and deadlines.
2) Reimbursement requests must be submitted to Accounts Payable and include the following:

a) A completed PRD including the appropriate departmental cost center or WBS element, GL and amount
b) Supporting documentation substantiating the reimbursement must include:
    1. Name of the company or person to whom payment was made (on a company letterhead, invoice or statement);
    2. Date expenditure incurred;
    3. Description of the goods or services performed;
    4. Purpose for which the goods or services were purchased; and
    5. Amount to be reimbursed.
c) See E-9 Compensation to Research Subjects for procedures related to reimbursement of expenditures research subjects.

e. Account reconciliations
Reconcile imprest accounts as follows:
1) The standard requirement is to reconcile the imprest fund and bank account at the end of every month. If operations warrant, reconcile more frequently (i.e., cash drawer operations). On a quarterly basis, submit a copy of the March, June, September and December reconciliation to Treasury Services by the 15th of the month following the reconciliation month.
2) Requests for overdue reconciliations will be sent by Treasury Services. The custodian's supervisor will be copied on a first request, the next level supervisor will be included on a second request, and Internal Audit will be notified on a third request.
3) Report any unusual activity, a change in custodian, or a change in fund status to Treasury Services.

f. Audits
All imprest funds must be reconciled and a copy of the reconciliation forwarded to Treasury Services as part of the annual audit. Treasury Services will notify custodians of the timing of the annual audit. Imprest funds are also subject to audit and/or random verification by Internal Audit, UK's external auditors and the Office of the Treasurer.

g. Extensions
The custodian may request to extend the repayment date by letter to Treasury Services.

h. Custodian change
1) Request a transfer of custodianship for an imprest cash fund by completing the Custodian Change Form.
2) A reconciliation of the fund must be performed and accompany the transfer request.
3) The custodian of record is not relieved of responsibility or accountability for the fund until the change is approved.

3. Closing an imprest fund
a. Request closure of the imprest fund when the original authorization period expires, the need for the fund no longer exists, or the custodian leaves the University.
b. The custodian must balance and replenish the fund to its original amount.
c. Once replenished, the custodian must prepare a cash or check transmittal to credit:

1) GL – 139000;
2) Fund – 0021700800; and
3) Notate on the transmittal the custodian's name and original DAV(s) or PRD(s) that issued the fund.

d. Treasury Services will confirm receipt and notify the University's financial institution to close any associated bank account.

4. Consequences of non-compliance
Misuse or improper accounting of the fund will, at a minimum, result in closing the fund.

IV. Security

A. Policy

1. Cash processing
All cash must be processed, stored and transported in a secure manner.
2. Level of Security- The level of security necessary at each cash handling location depends on the level of risk at that location. For example, the level of risk is generally higher at the central cash collection point of the University (i.e., Treasury Services) than in an academic department that only occasionally receives cash. To evaluate the level of risk at each location, the following factors should be considered:
   a. Amount of cash being handled;
   b. Geographic location;
   c. Hours of operation;
   d. Past loss experience; and
   e. Number and kinds of employees.

B. Procedures

1. General cash handling procedures
   a. Restrict access to areas where cash is counted or handled to persons directly involved and restrict visibility by the public in areas where large amounts of money are handled.
   b. Always keep doors locked in cash handling areas.
   c. Never leave cash unattended. This applies to cash registers and desktops. If an employee leaves his or her workstation for any reason, regardless of how briefly, appropriately secure cash in a locked place.
   d. Keep working funds to a minimum at all times. All other cash must be in a locked device.
   e. Reduce excess cash accumulated during the day by making more than one deposit per day.
2. Transporting funds
   a. Never send checks, cash or coin to Treasury Services via University or U.S. mail.
   b. Transport deposits to Treasury Services as follows:
      1) Armored car service: The University's armored car service transports money daily to and from major cash collection centers (e.g., Medical Center, Student Billings, and Athletics Association) to the University's bank. When requested by Treasury Services, armored car service transports deposits from specified locations directly to the bank (e.g., parking with large, heavy coin deposits).

2) Individuals: Individuals transporting cash must place it in bags, backpacks, etc., that are not obvious cash containers. If they are carrying large sums of cash they should be accompanied by another employee, but it is not recommended that individuals transport large sums of cash. If the level of risk is such that the department head believes there is a need for protection on an ongoing basis, or if he or she is unsure, he or she should contact Treasury Services.
3) Security guard: On an occasional basis, when large sums of cash need to be transported, the university's police department may be contacted to arrange a security guard escort.

3. Safekeeping devices
   a. Keep all cash in a safekeeping device that cannot be easily removed from the premises.
   b. Keep safe doors closed during business hours when the safe is in use, and locked when it is not in use. Keep safes locked at all other times.
   c. Other safekeeping devices (e.g., cash register drawers, cash boxes, bank bags containing cash) must be locked and secured when not in use. Do not secure personal cash and property in a University safekeeping device except for that belonging to patients in the University medical facilities.
   d. Control of safe combinations
      1) Give safe combinations to a minimum number of employees and only to those whose functions require access.
      2) When staffing levels permit, to prevent access to secured cash after normal business hours, no one employee should have access to both a key to a door to an office and the safe combination. Where staffing levels do not permit this preferred internal control measure, the supervisor must develop a plan and exercise control to maintain the proper level of security over cash.
      3) To the extent practicable, memorize safe combinations and do not write them down.
      4) Open safes in such a manner that no other person can observe and determine the combination. Change the combination when a person knowing it is no longer to have access to the safe.
   e. Each department having a combination safe must establish and maintain a record of each person given the combination, dates the combination was changed, and the reason for the change. Point of sale (POS) system and cash registers
      1) Keep all cash drawers, point of sale systems, and cash registers locked when not in use.
      2) POS systems and cash registers must have the following capabilities:
         a) Comply with Payment Application Data Security Standards (PA-DSS);
         b) Produce customer receipts;
         c) Automatically imprint consecutive numbers (e.g. receipt numbers, transaction numbers) on both the POS or register tape and the customer receipt; and
         d) Provide transaction display windows visible to both the customer and cashier.

f. Safes purchased after April 1, 2013, are required to have dual locking devices such as two keys, or a key and combination, to obtain entry.
   1) Different departmental employees will be issued copies of keys. If key and combination, no one employee will have access to both.
   2) No more than five and no fewer than two department employees will be issued keys or given the combination.
   3) Keys will be the property of the designated employees and under no circumstances are they to be stored in the department.

g. Opening and closing procedures of safekeeping devices must be followed:
   1) Two people must be present at all openings and closings of safekeeping devices, including the opening and counting of change orders received from the bank. The two people will initial a safe log that documents the safe's opening and closing activity, as well as the contents of the safe at close and open.
   2) If the unit cannot follow this control procedure because there is only one employee, the supervisor of the respective cash handling location must personally exercise control to maintain the proper level of security to minimize potential losses.

4. Overnight and after business hours safekeeping

An organizational unit receiving cash too late in the business day to prepare and deliver transmittals to Treasury Services, after armored car pickup, after normal business hours or on weekends may retain cash for safekeeping provided it follows the safekeeping procedures defined below:

a. Store all cash received after normal business hours in a safekeeping device.

b. Transfer of cash to a central location for safekeeping - In certain locations, cash (e.g., change funds) may be delivered to a central location for safekeeping after working hours. A transfer of cash for temporary safekeeping does not involve a transfer of responsibility for effective control of the cash. Standards for maintaining effective control include:
   1) Count all cash prior to deposit for safekeeping and again immediately upon return.
   2) Keep records of all transfer transactions, including receipts when cash is deposited and when it is recovered.
   3) Cash deposited for safekeeping must not be surrendered without verification of the identity of the person requesting the cash.
   4) Only containers that can be locked by key or combination, or are sealed, may be used for safekeeping.
   5) All containers used for safekeeping deposits must be labeled in such a way as to be individually distinguishable.
   6) Follow the transportation standards described earlier in this section when transferring cash for safekeeping.

c. If the unit receives more than $500 in cash after normal business hours or on weekends, consult Treasury Services for guidance on after hours deposit procedures.

5. Credit card transactions
   Credit Card transactions must be managed in an efficient manner and must comply with Payment Card Industry Data Security Standards (PCI DSS).[2] Security breaches can result in serious consequences for the University, including release of confidential information, damage to reputation, added compliance costs, substantial fines, possible legal liability and the potential loss of the ability to accept credit card payments.
   a. No University employee, contractor or agent who obtains access to payment card or other personal payment information in the course of conducting business on behalf of the University may sell, purchase, provide or exchange said information in any form to any third party other than to the University's merchant card processor, depository bank, VISA, MasterCard or other credit card company, or pursuant to a government request. This includes, but is not limited to,
      1) imprinted sales slips;
      2) photo or carbon copies of imprinted sales slips;
      3) mailing lists;
      4) electronic files or media obtained by reason of a card transaction.
   b. All requests to provide information to a party outside of the department must be coordinated with the Merchant Card Services Director in the Office of the Treasurer.
   c. Payment Card Industry Data Security Standards (PCI DSS) Compliance
      1) Merchant departments must comply with PCI DSS. These standards may be found at the PCI Security Council website (https://www.pcisecuritystandards.org/).
      2) Merchant departments may be subject to remote vulnerability network scans, server scans and application scans performed by the UK IT Security Office and approved third parties.
      3) Individual departments will be responsible for monetary sanctions and/or card acceptance restrictions imposed as a result of a breach in PCI compliance.
   d. Under no circumstance will credit card information be obtained or transmitted via email. Credit card information can only be stored or processed on individual computers or servers that have been deemed PCI compliant per Section VIII, Credit Card Payments. Credit card numbers submitted on hard-copy documents must be rendered unreadable and stored in a manner that would protect the individual cardholder information from potential misuse.
   e. Process for responding to a security incident
      In the event that a merchant knows or suspects that credit card data, including card number and card holder name, has been disclosed to an unauthorized person or stolen, the Merchant Department must immediately take the following steps:

[2] The payment card industry (VISA, MasterCard, Discover, American Express and JCB) has collaborated to create a single set of industry requirements, called the Payment Card Industry Data Security Standards (PCI DSS), for consumer data protection. PCI DSS aligns all payment card companies' security standards to create streamlined requirements, compliance criteria and validation processes. If a merchant does not comply with the security requirements or fails to rectify a security issue, the payment card industry may fine the responsible party, impose restrictions, or discontinue allowing the merchant to accept credit cards.

1) The MDRP or any individual suspecting a security breach must immediately call the Merchant Card Services Director.
2) If an actual breach of credit card data is confirmed, the Merchant Card Services Director will alert the merchant bank, the University of Kentucky Police Department, the Legal Office, the Office of the Treasurer, the Director of Internal Audit, the Director of IT and any relevant regulatory agencies of the breach.

V. Banking Relationships and Establishing Bank Accounts

A. Policy

1. University Financial Services
   Only the Treasurer of the University is authorized to establish bank accounts in the name of the University and its affiliated corporations and be the designated signatory authority for the disbursement of funds. No individuals, departments, administrative offices, or affiliated organizations of the University of Kentucky may establish a bank account or deal directly with a bank or similar depository institution for the purpose of making deposits, arranging for safekeeping of assets, cashing checks, or any other function without the written consent of the Office of the Treasurer.
2. University name and "marks"
   Bank accounts using the name University of Kentucky, or its "marks" (e.g., UK, U of K or similar abbreviations) and/or utilizing the University's tax identification number may only be established upon written approval of the Office of the Treasurer.

B. Procedures

1. Obtaining approval to open accounts
   To request authorization to establish an outside banking account or relationship for University activity, a written request must be sent to the Office of the Treasurer and contain the following information:
   a. Full name for the proposed title of the bank account (e.g., Professor, Custodian, Department, and University of Kentucky);
   b. Purpose of bank account;
   c. Amount of the original deposit; and
   d. Approval of the appropriate college or unit business officer.
2. Units that deal directly with banks
   Organizational units that have approval to establish an outside banking account must follow the below procedures:
   a. Deposit all cash in accordance with the daily deposit policy.
   b. Keep records of all cash receipts.
   c. Use a bank deposit slip when depositing cash.
   d. Obtain a certification of the deposit from the bank teller (e.g., a printed receipt from the bank or a stamped copy of the deposit ticket).
   e. Reconcile outside bank accounts monthly and make copies of the reconciliations available to the Office of the Treasurer or Internal Audit, as requested.
3. Related organization bank accounts
   Related organizations, such as student organizations, may have bank accounts under the following conditions:

a. They cannot use the University's tax identification number (TIN) on the account. The social security number of the organization's treasurer or the organization's own TIN must be used in lieu of the University's TIN.
b. Related organizations cannot use the University's name or related "marks" (e.g., UK, U of K, or similar abbreviations) without obtaining prior approval of the appropriate University business officer and the Treasurer. To request use of the University's name or related "marks" please complete the form titled *Related Organization Request To Open Bank Account Using University's Name and/or "Marks".*
c. Checks payable to the University of Kentucky must not be deposited into the bank account.
d. An annual summary of deposits and disbursements transacted in the bank account must be provided to the University's Treasury Services Department.
e. Bank statements, deposit and disbursement records must be maintained for a minimum of three years to facilitate periodic review or audit by the University.

VI. Personnel Related Issues

A. Hiring considerations for cash handling positions

1. All job requisitions used to post positions that have cash handling responsibilities need to include these responsibilities in both the job summary and position access sections of the job requisition.
2. Before hiring an external individual, the hiring official must submit background check requests, including educational verification, employment verification and a criminal history check, to Human Resources per Human Resources Policy and Procedure Number (HRP&P) 11.0: Pre-employment Screening. Human Resources will consult with the hiring official as to any relevant considerations before an offer of employment is made.
3. When hiring an internal individual, the hiring official must verify prior employment with any previous University department.

B. Cash Handling Guidelines

1. All employees, including supervisors, are required to read this manual and the Cash Handling Quick Reference Guide then sign the Cash Handling Form.
2. Departments are encouraged to modify the guide and form to include procedures unique to the unit.
3. Retain the original form in the departmental personnel file and give a copy to the employee.

C. Training

1. Handling cash and cash equivalents
   All employees working in cash and cash equivalent operations must be provided with periodic training that reviews University policies and procedures as well as departmental internal procedures and receive specific training on cash handling procedures outlined in the Treasury Operations Manual.
2. Accepting credit card payments and PCI DSS training
   PCI DSS requires all employees involved in processing credit card

transactions to be aware of policies and procedures concerning the safeguarding of cardholder data. As part of the university PCI DSS compliance program, all merchant units must follow the guidelines below.

a. When a new merchant account is established, the MDRP of that merchant unit must attend the next available PCI DSS training course, scheduled on an as needed basis.
b. All MDRP's of university merchant units must attend an Annual PCI DSS Compliance Training session, usually held each fall.
c. Each merchant unit must be able to provide documentation that each employee involved in the processing of credit cards has read and agrees to comply with the unit's PCI DSS policy and procedures, the sections pertaining to credit card processing within the Treasury Operations Manual (E-2-1), and any other PCI DSS training materials available to them at the time.

D. Corrective action and separation from employment

1. The University considers violations of policies and procedures of the Treasury Operations Manual a serious failure on the part of the employee and the supervisor. Appropriate corrective action must be taken in accordance with HRP&P #62:0 Corrective Action.
2. Violations of the policies and procedures of the Treasury Operations Manual that are deemed by management to be severe or repeated violations are considered grounds for termination of employment as outlined in HRP&P #12:0 Separation from Employment.
3. Employees charged with theft of university funds will be suspended pending conclusion of the investigation. If the investigation finds sufficient cause for officials to believe theft has occurred, employment will be terminated and criminal charges will be filed.

VII. Reporting Losses

A. Policy

All losses of University cash and securities, including those for which the University has legally accepted custody and responsibility, must be reported, regardless of the cause and amount. This includes losses from actual or suspected theft, burglary, or robbery; errors in record keeping or making change where theft is not suspected; acceptance of invalid or nonredeemable paper, including forged or altered checks; or acceptance of counterfeit money.

B. Procedures

1. Reporting Losses
   a. Report all losses immediately to the supervisor of the department, administrative office, or affiliated organization. The supervisor must make a written report of each loss and send a copy of the report to Treasury Services.
   b. For losses more than $100, also send a copy of the report to Treasury Services, campus police (local police for out-of-town locations), Internal Audit, and Risk Management.
   c. University employees may only make statements regarding a loss to a member of the following:
      1) Police;

2) Treasury Services;
3) Risk Management;
4) University Financial Services;
5) Internal Audit; or
6) University Legal Counsel

d. Contact Treasury Services for instructions on accounting for losses.

2. Attempted theft
Attempted theft, burglary, or robbery should be reported immediately to the department supervisor and the campus police (local police for out-of-town locations), even though no actual loss occurred.

VIII. Credit Card Payments

A. Policy

Credit card payments may be processed via credit card swipe terminals, POS systems, through the UK websites using a hosted order page from a third-party internet payment gateway vendor or other approved payment applications. Credit card transactions must be managed in an efficient manner and must comply with Payment Card Industry Data Security Standards (PCI DSS). These standards ensure that credit card activities are consistent, efficient and secure for all types of credit card activity transacted, whether in-person, over the phone, via fax, mail or the Internet. These standards may be found at the PCI Security Council website (https://www.pcisecuritystandards.org/).

B. Procedures

1. Process to implement acceptance of credit card payments
The Merchant Department Responsible Person (MDRP) must take the following steps to implement payment card processing at the University.
   a. Read these procedures thoroughly.
   b. Complete and sign the Application to Become a Merchant Department. https://www.uky.edu/hr/sites/www.uky.edu.hr/files/eForms/MerchantApplication.pdf
   c. Forward the application to the Dean/Director or Chair as appropriate for approval.
   d. Submit the application to the Merchant Card Services Director.
2. Equipment and supplies
   a. Equipment (i.e., swipe terminals or manual imprint machines) for processing credit cards must be PCI compliant and will be acquired by coordinating with the Merchant Card Services Director. Any equipment no longer being used to process credit card transactions must be returned to the Merchant Card Services Director.
   b. Point-of-sale (POS) systems and cash registers must be certified as PA DSS compliant.
3. Software and e-Commerce
   a. Any department with a need to accept credit cards through the internet via a web application (e-Commerce) must contact the Merchant Card Services Director to coordinate web-based payment solutions with the payment processor under contract with the University.
      1) Merchants must use a hosted order page model where the credit card information is collected and processed by a validated PCI

DSS compliant third-party internet payment gateway service provider.

2) All third party service providers involved in the processing of internet-based ecommerce credit card transactions will need to provide documentation of PCI DSS compliance, as well as be listed on the VISA Global Registry of PCI DSS Validated Service Providers (https://www.visa.com/splisting/index.html).

b. Server-based software applications that collect and transmit credit card data for payment must be certified PA DSS compliant and listed on the PCI SSC List of Validated Payment Applications. Any department interested in implementing a server-based software application or POS system to accept credit card payments must consult with the Merchant Card Services Director to ensure PCI DSS compliance.

4. Card association rules and regulations
Visa, MasterCard, American Express and Discover are the only credit cards that may be accepted. Merchant Departments are expected to comply with the rules and regulations set forth by each of the card associations in the processing of credit card payments. Each card association's rules and regulations can be found on their company websites, or you can request a copy from the Merchant Card Services Director. The card associations may impose fines or revoke the privilege of accepting credit cards for not complying with their rules and regulations. The following card association rules are noteworthy and must not be violated by a University Merchant Department:
   a. No minimum credit card transaction amount may be set.
   b. You must accept a credit card as payment unless the transaction cannot be authorized.
   c. If you require additional information, such as a driver's license or phone number, do not record the information on the sales draft.
   d. Refunds for purchases made by credit card must be made by crediting the original card, not by cash or check.
5. Credit card processing costs - Merchant Departments are responsible for all costs associated with the acceptance of credit cards including costs of supplies and equipment, as well as processing fees. Departments are also responsible for any credit card transactions that are disputed and charged back to the University.
6. Accounting for transactions
   a. Process for posting credit card payments
      1) At the end of the day, the credit card terminals, POS systems and internet payment gateways settle, either automatically or manually, all transactions processed throughout the day by transmitting the settlement batch to the credit card processor for collection of those transactions.
      2) On the following business day (the 2nd day), the credit card processor generates an ACH for the total of each settlement batch to be sent to the university restricted trust account.
      3) On the next business (the 3rd day), the ACH transactions for all settlement batches for all university merchants are received at the university bank.

4) Treasury Services will upload those ACH settlement amounts into SAP, posting the settlement amount to the cost center listed on the merchant application for each university merchant.
5) Credit card settlements can only be posted to a single cost center for a single merchant, thus settlements cannot be split amongst multiple cost centers.
6) The merchant departments must reconcile the credit card activity posted to the general ledger.

b. Each merchant department will receive monthly statements directly from the University's credit card processor for reconciliation purposes and must verify that the information on the merchant statement is correct.

7. Review of merchant processes
Merchant Services will coordinate periodic reviews of merchant departments. Merchant Departments not complying with approved safeguarding and processing procedures may lose the privilege of serving as a credit card merchant.
8. Changes to merchant account
Merchant departments must notify the Merchant Card Services office prior to making any changes to their method of processing after the merchant has been initially set up by completing and submitting a Merchant Account Termination/Change Form. Examples of changes that require the completion of this form include changing from terminal based processing to processing through PC software or through a Web site, changes to business processes, or changes in personnel related to the account.
9. Termination of merchant account
   a. If a merchant department no longer wishes to accept credit cards, the MDRP must complete the Merchant Account Termination/Change Form and submit it to the Merchant Card Services Director.
   b. Any equipment (i.e. swipe terminals or manual imprint machines) associated with the terminated merchant account must be returned to the Merchant Card Services Director.
10. Security
Credit card transaction must be processed in a secure and safe manner pursuant to Section IV, Security.

C. Other Reference Materials

PCI DSS and UK (http://www.uky.edu/ufs/merchant-card-services-pci-dss)

VISA (https://usa.visa.com/support/small-business/security-compliance.html)

MasterCard (http://www.mastercard.com/us/sdp/index.html)

Discover (http://www.discovernetwork.com/fraudsecurity/disc.html)

Payment Card Industry Security Standards Council
https://www.pcisecuritystandards.org/index.php

VISA Global Registry of PCI DSS Validated Service Providers
(http://www.visa.com/splisting/index.html)

PCI-SSC List of Validated Payment Applications
https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

American Express Data Security
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home&ln=en&frm=US