Table of Contents

1. Purpose. To set forth the regulations and procedures governing the collection of cash, the use of change and petty cash funds, and to establish and define requirements for collecting, storing, processing and transmitting credit card data to ensure proper control and integrity of data as well as to facilitate compliance with PCI DSS requirements. These standards are designed to assist Washburn in the safekeeping of cardholder information, which in turn reduces the chances of security breaches, fraud, and potential financial losses.

2. Definitions. For the purpose of these regulations and procedures the following definitions apply.

2.1 "Cash" means coins, paper currency, checks, money orders, and debit and credit card authorizations.

2.2 "Cash Collections" means cash collected by a Department, University committee, Employee group, or Student group.

2.3 "Cash Funds" means cash collections, change funds, and petty cash funds collectively.

2.4 "Change Fund" means a specific amount of cash set aside for making change during cash collections activities.

2.4.1 "Temporary Change Fund" means a fund established for a short-term purpose or event that must be returned to the Business Office within an agreed upon timeframe.

2.4.2 "Permanent Change Funds" means a fund that will remain within the designated department for ongoing cash collection activities.

2.5 "Petty Cash Fund" means a specific amount of cash reserved for small expense reimbursements.

2.6 "Payment Card Industry Data Security Standard (PCI DSS)" means a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations that hold, process, or pass cardholder information.

2.7 "Cardholder Data" is any personally identifiable data associated with a cardholder. Examples include but are not limited to: account number, expiration date, card type, name, address, social security number, and Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card referred to as CVV2 or CVC2).

2.8 "Merchant ID number (MID)" is a unique number that identifies each department for accounting purposes. Point of Sale (POS) is a computer or credit card terminal that either runs as a stand-alone system or connects to a server at the University or at a remote offsite location.

3. Security of Cash Funds.

3.1 Cash Box. All non-deposited cash funds shall be maintained in a locked cash box. When not in use, the cash box shall be kept in a secure, locked place, such as a fireproof safe or fireproof filing cabinet. Funds of $1,000 or over shall be stored in a fireproof safe.

3.2 Storage Location Restriction. Cash funds shall be secured only in University buildings. Cash funds shall not be taken to or stored in a private residence, University housing, or motor vehicle.

3.2.1 Arrangements may be made with the University Police Department to safeguard the cash until the Business Office is open. Contact the University Police Department for additional information.

3.3 Audit Procedures. All cash funds are subject to audit by the Business Office or other Department performing internal audit functions, as well as by the external auditors. Audits may be either scheduled or unannounced.

3.3.1 All receipts not yet submitted to the Business Office shall be retained for reference during audits.

3.4 Loss of Cash Funds. Losses shall be immediately reported by the custodian of the funds to the Department Head, the Director of Accounting, the Bursar, and the University Police Department.

3.4.1 A complete investigation and report shall be made of the circumstances involved.

3.4.2 The Department budget shall be charged for the amount of the loss up to $500 when required documentation and security procedures were in place at the time of a theft or mysterious disappearance of cash.

3.4.3 The remaining portion of the loss may be charged to the Department budget if the investigation finds required documentation and/or security procedures were not in place.

3.5 Custodian Responsibility for Loss. The custodian of the funds may be held personally responsible for some or all of a cash fund loss. Reimbursement by the custodian may be required if one or more of the following conditions are identified:

- The collection activity or the change or petty cash fund was not authorized by the Bursar or Director of Accounting;
- A specific cash fund was commingled with personal funds, or another cash fund;
- Current, complete records of cash fund activity were not maintained;
- Cash fund was not properly secured;
- All cash collected was not accounted for and reconciled to deposits;
- Cash collected was not deposited with the Business Office on a timely basis;
- Expenditures were made from non-deposited cash collected;

- Payments have been made from the petty cash fund without obtaining an original receipt; or,
- Payments have been made for purposes for which the change fund is not authorized. Such purposes include, but are not limited to, personal check cashing, travel advance, lunches, or payment of personal expenses.

3.6 Loss of Personal Funds. A loss of personal funds should be reported to the University Police Department.

3.6.1 Neither individuals nor Departments will be reimbursed for loss of personal funds.

3.6.2 Personal funds include:

- Unauthorized petty cash funds;
- Unauthorized Department cash collections;
- Unauthorized change funds; and,
- Flower funds, coffee funds, and other similar funds.

3.6.3 If there is a question whether the funds are personal or University funds, contact the Director of Accounting.

4. Cash Collections—General. Cash collections occur in activities including, but not limited to, sales of goods or services, social events, and admission ticket sales.

4.1 Cash Collections Approval. Cash collections by any University Group requires approval by the Bursar or Director of Accounting.

4.2 Course Fees and Supply Charges. No Department may establish or collect separate course, laboratory or other fees, or charge Students for the cost of supplies without prior approval from the Administration. Any such fees or charges must be posted to Student accounts and collected in the Business Office.

4.3 Deposits. Cash collections shall be deposited in the Business Office as outlined below:

4.3.1 If cash is collected during normal business hours, the deposit shall be made on the day of receipt.

4.3.2 If cash is collected when the Business Office is closed (for example, weekends and holidays), the deposit shall be made the next business day.

4.3.3 Daily deposits may not be required when the amount to be deposited is less than $50. In such case, the deposit shall be made by the close of business of that workweek.

4.3.4 When cash collections are not deposited on the day of receipt, the security procedures outlined in Section 3 above shall be followed.

4.4 Expenditure Restriction. No expenditures shall be made from non-deposited cash collections.

4.5 Donor Contributions. Normally, donor **c**ontributions made to the University are deposited with the Washburn University Foundation. Please utilize the appropriate Foundation form for the deposit.

4.6 Responsibility. Individuals responsible for accepting cash collections may be held personally liable for shortages of funds occurring through theft, loss, or improper disbursement.

5. Cash Collections—Procedures.

5.1 Departmental Collection of Cash. All Department cash collections involving University resources shall be deposited in the Business Office and credited to a University account.

5.2 Point of Sale Procedures.

5.2.1 Checks accepted for payment are to be made payable to WASHBURN UNIVERSITY and immediately stamped "FOR DEPOSIT ONLY".

5.2.2 Departments are not authorized to cash checks.

5.2.3 Individuals receiving cash shall:

- Use pre-numbered receipt forms when applicable and when feasible to do so; exceptions include but are not limited to bake sale, raffle, and similar transactions.
- Indicate on the receipt the date, customer's name, services rendered, or items purchased, and amount of the sale. Use a separate line to indicate Kansas sales tax collected (if applicable);
- Provide a copy of the receipt to the customer;
- Provide a copy of the receipt to the Business Office together with the Department deposit form and cash collected; and,
- Retain a copy of the receipt in a Departmental file.

5.2.4 Any other method of recording cash collections is subject to approval by the Director of Accounting prior to implementation.

5.2.5 Tickets may be sold for admission to events. A ticket report shall be prepared which:

- Accounts for the range of tickets issued for an event; and,
- Is reconciled to the total of cash deposited in the Business Office.

5.3 Deposits.

5.3.1 Two copies of the Deposit form (available online) specifying the FOAPAL shall be completed (See Section 5.2.3 above). The sales tax collected shall be recorded in a sales tax liability account.

5.3.2 Included with deposits shall be a listing attached to the copies of the pre-numbered receipts. The list is to document the total amount:

- Of goods or services sold, excluding sales tax;
- Of sales tax collected; and,
- Being deposited.

5.3.3 If a duplicate deposit form is provided (see 5.3.1 above), the Business Office will return to the depositor one copy of the deposit form as a receipt documenting the validated total of the deposit.

5.3.4 The Business Office will retain one copy of the deposit form. This deposit receipt and any attached items shall be scanned and saved by the Business Office to be available for audit.

6. Procedures Common to Petty Cash and Change Funds.

6.1 Ownership of Cash Funds. All authorized cash funds are University property. Such funds shall be:

- Utilized only for the purposes described in Sections 7 and 9 below; and,
- Subject to the appropriate handling and accounting procedures adopted by the Administration consistent with generally accepted accounting practices.

6.2 Specific Regulations. See Sections 7 through 10 below for regulations and procedures specific to each type of cash fund.

6.3 Request to Establish Fund. To establish a cash fund, submit a completed "Change Fund Application" form to the Bursar. The dynamic form may be obtained from the Finance office SharePoint site.

6.3.1 Approval or denial shall be by the Bursar or Director of Accounting. The requesting party shall be notified of the approval or denial. Denied requests may be appealed to the VPAT.

6.3.2 Non-approved cash funds are subject to forfeiture to the University General Fund.

6.4 Obtaining Approved Fund.

6.4.1 If a cash (petty or change) fund is approved, amounts $200 or less may be obtained at the Cashier window in the Business Office. For amounts over $200, a dynamic form

payment voucher should be submitted with the approved Petty Cash/Change Fund Application for Accounts Payable to create a check.

6.4.2 The check or cash shall be picked up at the Business Office Cashier window by the custodian of the fund. The top portion of the "Custodial Record" form shall be completed by the custodian before the check is released.

6.5 Termination or Reduction of Cash Funds. See sections specific to each of the cash fund types.

6.6 Transfer of Custodial Responsibilities. To transfer responsibility for a cash fund, send an email from your Washburn email to business-office@washburn.edu with the new custodian on copy.

6.6.1 A copy of email transfer request should be retained in the department to be available for audit.

7. Petty Cash Fund—General.

7.1 Petty Cash Fund Need. A petty cash fund may be established when:

- A Department has a need to make frequent purchases of less than $25.00; and,
- Vendors will not accept procurement cards or allow merchandise to be charged to the University.

7.2 Petty Cash Fund Restricted Use. Petty cash funds shall not be used to:

- Pay Employees or independent contractors for services rendered to the University;
- Pay for any travel, meals, or entertainment expenses;
- Make loans to any individual, group or entity. For purposes of these regulations, "loans" include, but are not limited to, IOU's, notes, post-dated checks, or checks presented for cash, but not deposited by the next business day; or,
- Pay any expense incurred for a non-University business purpose.

7.3 Petty Cash Fund Centralized Administration. The administration and accounting of petty cash funds shall be centralized within a Department.

7.4 Petty Cash Fund Termination. The VPAT, AVP Finance, Director of Accounting, or Bursar may terminate a petty cash fund when:

- Infrequent use of the fund warrants termination;
- There has been a violation of petty cash handling policy, regulations, or procedures;
- The Department requests termination of the fund; or,
- The fund will not be used for 30 days or more.

7.5 Reduction of Petty Cash Fund. The VPAT, AVP Finance, Director of Accounting or Bursar may reduce a petty cash fund when:

- Monthly expenditures from the fund average less than 1/3 the amount of the fund. Example: A $100 fund averaging expenditures less than $33.00 per month would be subject to reduction; or,
- The Department requests reduction of the fund.

7.6 Voluntary Petty Cash Fund Termination Procedure. To terminate a Petty Cash fund the department or custodian of the fund shall:

- Prepare a payment voucher for an amount equal to the receipts not yet replenished to the fund;
- Provide an explanation when the cash amount plus voucher amount does not equal the total authorized for the fund;
- Complete the bottom portion of the "Custodial Record" form; and,
- Deliver the cash balance on hand, all receipts, and the "Custodial Record" form to the Business Office.

8. Petty Cash Fund—Departmental Procedures.

8.1 Receipt for Petty Cash Purchases. An original receipt shall be obtained for each purchase made and shall be signed and dated by the person making the purchase.

8.2 Petty Cash Fund Replenishment. The fund shall be replenished in amounts equal to the total of submitted receipts. To replenish the fund, the custodian of the fund shall submit a payment voucher to Accounts Payable with original receipts attached. Accounts Payable will issue a check for the amount of the payment voucher that can then be cashed to replenish the fund.

8.3 Petty Cash Fund Bookkeeping. The custodian of the fund shall maintain a permanent, continuous ledger documenting fund transactions. The ledger may be paper or electronic and shall:

- Show every expenditure made;
- Show every replenishment received from the Finance Office;
- Allow easy determination of cash on hand by keeping a running balance; and,
- Show the amount not yet replenished by the Finance Office.

8.3.2 The ledger and receipts shall be retained separately from the cash box.

8.3.3 The following petty cash fund ledger format is recommended:

Date	Transaction	Expenses	Receipts	Balance
09/15/06	Establish petty cash fund		$50.00	$50.00
09/27/06	Postmaster-stamps	$3.70		$46.30
10/09/06	Kinko's	$12.25		$34.05
10/13/06	Office Max	$23.50		$10.55
10/15/06	Finance Office replenishment		$39.45	$50.00

9. Change Fund—General.

9.1 Change Fund Usage. A change fund is established to make change at locations where sales are made involving cash and can be either Temporary or Permanent. Change funds shall not be used to:

- Pay expenses of any kind;
- Provide reimbursement for any expenditures;
- Make loans of any type. Loans include, but are not limited to IOU's, notes, post-dated checks, or checks presented for cash but not deposited by the next business day; or,
- Cash personal checks.

9.2 Change Fund Termination. The VPAT, AVP Finance, Director of Accounting, or Bursar may terminate a change fund when:

- The Director of Accounting or Bursar determines the fund is inactive;
- The Director of Accounting or Bursar, determines there has been a violation of change fund handling policy, regulations, or procedures; or,
- The individual(s) responsible for the fund requests closure.

9.3 Change Fund Reduction. A change fund shall be reduced if one or more of the following circumstances exist.

- The Director of Accounting or Bursar determines activity of the fund warrants a reduction; or,
- The individual or individuals responsible for the fund request a reduction.

9.4 Change Fund Termination Procedure. The following applies when a change fund is to be closed:

- The cash shall be delivered to the Business Office;
- The amount of fund shortage, if any, shall be charged to the Department budget;

- The amount of fund overage, if any, shall be credited to University miscellaneous income; and,

- If available, the custodian of the fund shall complete the bottom portion of the "Change Fund Custodial Record" form.

9.5 Change Fund Custodian Responsibility. The custodian of the fund may be held responsible for a change fund loss. If so, the custodian may be required to reimburse the University. This would apply when investigation reveals one or more of the following:

- The fund has not been properly registered with the Business Office;
- The fund has been commingled with revenue collected by the Department that should have been deposited with the Business Office;
- The fund has been commingled with personal funds or petty cash funds;
- An on-going record of activity has not been maintained;
- The fund has not been properly secured; and,
- Payments have been made for purposes for which the change fund is not authorized. Such purposes include, but are not limited to: personal check cashing, travel advances, lunches, or payment of expenses.

10. Credit Card—Procedures.

10.1 Credit Card payments must be processed in compliance with Payment Card Industry Data Security Standards (PCI DSS) which are intended to limit exposure and/or theft of personal cardholder information.

Washburn must adhere to these standards in order to retain our ability to accept credit card payments. Departments not complying with approved safeguarding, storage, processing, and administrative procedures will lose the privilege of accepting and/or processing credit cards. In addition, each department engaged in credit card processing may be held responsible for any financial losses due to poor or inadequate internal controls or negligence in adhering to the PCI Standard

10.2 "Scope". This procedure applies to all University employees, faculty, students, contractors, guest, consultants, temporary employees, volunteers, and any other users who accept donations or sell goods, services, or information, and accept credit cards as a form of payment.

All computers and electronic devices used for processing payment card data are governed by PCI DSS. This includes servers that store payment card numbers, workstations that are used to enter payment card information, and computers or credit card swipe devices through which payment card information may be transmitted.

10.3 "Department Responsibilities". Departments are responsible for knowing and complying with PCI DSS and University policies, regulations, and procedures to safeguard credit card and other personally identifiable or sensitive information. Departments must also

follow established procedures to ensure that cardholder information is handled and stored securely. This applies to all transactions regardless of the type of transaction (phone, in-person, mail, web, etc.).

10.4 "Establishing Payment Card Services". Any University department wishing to accept credit cards for goods or services must first contact the Bursar (Business Office) who will work with departments to determine a solution that best fits the department's needs in terms of credit card processing. The preferred solution is through E-Commerce (see below), but other options can be explored. Once a solution has been chosen, the Business Office may develop a process to use an existing Merchant ID Number (MID) or request a new MID. In order to accept credit card payments, departments must first have a MID.

All transactions that involve the transfer of credit card information must be performed on systems approved by ITS and the Business Office and will include a compliance and security review. Approval MUST be obtained prior to entering into any contracts or purchases of software and or equipment relating to credit card processing. This requirement applies regardless of the transaction method or technology used. There are several approved University methods to accept credit cards, including e-commerce, in person via web-based virtual terminal, or via a Point of Sale (POS) terminal connected to the Internet.

Departments may not set up their own banking relationships for payment card processing. Payment card revenue must be deposited into designated University bank accounts. PayPal, Venmo, and accounts of a similar type are not University-approved bank accounts.

10.5 "E-Commerce Transactions". TouchNet is the University's primary credit card processing application and to the extent possible, is to be used for all online credit card transactions. This type of transaction begins when the customer purchases a product, registers for an event, or makes a donation, etc., through a payment application website. In this situation, the customer is not present for the sale. TouchNet offers a variety of solutions that have been configured to meet the PCI Data Security Standards. The Business Office will work with Departments to determine the appropriate E-Commerce solution.

10.6 "Point of Sale Transactions". Some departments may have specialized software or a Point of Sale (POS) system for processing credit cards. Payments may be processed with the cardholder present or cardholder not present by mail, telephone, or fax order per the department's business operational needs. The credit card transaction process begins when the customer purchases a product and their card is tapped, dipped, swiped or entered into a point-of-sale system.

10.7 "Processing Transactions". Specific details regarding processing and reconciliation will depend upon the method of credit card acceptance and type of merchant account. Detailed instructions will be provided when the merchant account is established. Only authorized individuals can process credit card transactions.

10.8 "Card Reading". If the credit card is present it may be inserted or tapped using an EMV chip. The EMV chip method of reading card information is generally the least expensive and most secure because it produces a unique code for each transaction that is more

difficult to steal. If a card is swiped in the reader using the magnetic strip on the back of the card, the transaction fees are charged at a higher rate and the transaction is considered less secure. Both methods of processing credit cards eliminate the need to manually enter the credit card information.

All device surfaces should be periodically inspected to detect tampering and unauthorized substitution. Departments with card readers should be aware of the following:

- Pay attention to and follow up on suspicious behavior around devices.
- Report suspicious behavior and indications of device tampering or substitution to appropriate personnel.
- Verify the identity of any third-party persons claiming to be repair or maintenance personnel before granting them access to modify or troubleshoot device.
- Follow procedures to ensure devices are not installed, replaced, or returned without verification.

10.9 "Manual Key Entry." If the credit card is not present, the credit card information may be entered manually but strict adherence to guidelines on handling card information is required. Information needed to enter manually will be the credit card number, expiration date, amount to be charged, CVV code and the billing zip code. The CVV and billing zip code will ensure a lower rate for processing the transaction.

10.10 "Daily Settlements". Systems must be closed out daily and reconciled to the daily activity to ensure all transactions are correct. The daily batch settlement report is generated when the system is closed each day. The bank charges a higher processing fee for any transactions that are not settled daily.

10.11 "Security of Cardholder's Information". Cardholder information is obtained either by the cardholder being present (credit card present) or by transmitting cardholder information (telephone, internet, etc.). All individuals authorized to accept credit card payments must securely process, store and dispose of credit card data in order to adhere to the Payment Card Industry (PCI) Data Security Standards (DSS).

Credit card numbers must be masked in reports or settlements to protect account information for all users except those who have a legitimate business need. The first six or last four digits are the maximum number allowed to be displayed.

If any card information is written down while performing the transaction, that information must be shredded once the transaction has been completed. If credit card information is obtained and recorded for future use (example: periodic billing for partial payments), the information must be secured and not accessible to unauthorized individuals (safe, locked file cabinet, etc.). There are additional PCI requirements such as logging and auditing of access to data. Materials must be stored in secure storage containers prior to destruction; once used the materials must be properly destroyed by cross-cut shredding, incineration, or pulping so that cardholder data cannot be reconstructed.

It is not permissible to transmit or obtain credit card information by email, wireless devices, PDAs, instant messaging, Chat applications or other unsecure methods unless otherwise approved by ITS and the Business Office. If email containing cardholder data is received, immediately delete the email from all folders and notify the sender that the University does not accept cardholder data via email and that the transaction will not be processed. In the response, give the customer alternative methods of payment for sending cardholder data (by telephone or through TouchNet). If you reply to the original email, make sure you remove any card information before sending the message. Also, be sure to delete the message from your email inbox, sent box, and deleted box.

Report any suspected exposure (to unauthorized parties) or loss of cardholder data to ITS and the Business Office immediately. This includes lost or stolen files with credit card numbers, electronic loss of data, databases infected with viruses and any other loss or potential loss.

11. Assistance. Direct questions concerning:

- University accounting policies and procedures to the Director of Accounting or Bursar;
- Cash fund procedures to the Bursar; and,
- The security of cash funds to the University Police Department.