



# Department Administrative Policy and Procedure

**Subject:** Receipt and Handling of University Funds

**Number:** UW DAP 7-9.1

---

## I. PURPOSE

To establish procedures that create controls through the University of Wyoming (University) departments in order to safeguard against the loss of funds and help discharge the University's financial responsibilities when handling funds.

## II. DEFINITIONS

**Funds:** Funds include currency (paper banknotes), coins, checks (including personal or business checks, cashier's checks, certified checks, and electronic or e-checks), money orders, cryptocurrency, credit card transactions, and other similar financial instruments. Funds received on behalf of the University include, but are not limited to, departmental collections for programs and activities (including ticket sales), collections as a result of the use of campus equipment and facilities, collections for services provided by University employees related to their employment<sup>1</sup>, collections for the on and off campus sales of goods, collections for services of University departments, and donations.

**Payor:** Individual submitting funds to the University for any purpose other than a contribution, donation, or gift.

**Postdated Check:** A check with a date later than the date the Payor presents it for payment to the University.

**Third-Party Check:** A check written by the owner of the check to the Payor presenting it to the University, i.e., the Payor is signing the check written to the Payor over to the University rather than cashing the check and presenting the funds to the University.

**Two-Party Check:** A check made payable to more than one party. A check payable to the University and the receiving University Department is not considered a Two-Party Check.

---

<sup>1</sup> This does not include Compensated Professional Services which includes outside compensated work or scholarly services performed by a University Employee. Provision of Compensated Professional Services is recognized as a legitimate activity unless specifically prohibited by an Employee's contract of employment. Compensated Professional Service is not considered appropriate when it interferes with the regular work of the University Employee; involves unauthorized use of University facilities, personnel, or other resources; or unfairly competes with private sector companies. (See W.S. 9-2-3220(b)(viii)).

### **III. POLICY**

**All funds of the University of Wyoming are public funds** and are intended to help accomplish the mission of the University and its units. It is the responsibility of all employees to safeguard University assets. It is the responsibility of all officers, deans and department heads to ensure that adequate internal controls within their units exist and are observed.

This Policy is not intended to be all-inclusive. It is intended that the principles discussed will provide procedures applicable to most fund receipt and handling situations. Additional information can be found in the [Standard Administrative Policy and Procedure Receipt and Handling of University Funds](#) and assistance is available from all UW Financial Affairs departments, specifically the Associate Vice President of Finance Office, the Cashier's Office and the Accounting Office. Risk Management, Internal Audit, and the University of Wyoming Police Department can also provide valuable information as needed.

#### **A. Receipt and Deposit of Funds.**

1. All funds received on behalf of the University that do not qualify as a Contribution, Donation, or Gift must be acknowledged by receipt when received. The University recipient of funds from a Payor must retain a copy of the receipt.
2. All funds collected by departmental personnel in the performance of assigned duties are considered University public funds and must be deposited intact with the Cashier's Office or other respective office per Appendix D. All funds must be ultimately routed to the Cashier's Office, Office of Sponsored Programs, or Accounting Office as indicated in the table provided in Appendix D for deposit into UW's bank account. Some specifically outlined deposits are required to be remitted to the Procurement and Payment Services Office or Office of Scholarships and Financial Aid to internally process the receipt prior to submission of the deposit to the Cashier's Office
3. Individual departments and programs may not establish a bank account or otherwise withhold University funds from deposit into official University accounts.
4. Donations, contributions and gifts to the University are properly deposited to and retained by the University of Wyoming Foundation (Foundation). Foundation financial personnel should be consulted in the event a gift is received directly by a campus department.

#### **B. Basic Elements of Receipt and Handling of University Funds.**

1. **Receipt processes and documents.**

- a. Receipt records must be prepared at the time funds are received to provide revenue accounting and reconciliation with actual funds collected necessary for program management and tax reporting purposes.
- b. Multi-copy receipting systems such as electronic cash register receipts or pre-numbered handwritten receipts are acceptable forms of receipt documents.
- c. The Payor should be given the original pre-numbered receipt if a receipt book is used. The carbon copy should be left in the book.
- d. For retail sales, cash register receipts should be given to the Payor.
- e. For ticket sales, the pre-numbered ticket given to the Payor is the receipt and no other receipt is necessary.
- f. For concessions or vending sales, receipts are not required to be given to the Payor.
- g. Direct deposits to University bank accounts are exempt from the receipt requirement.
- h. Checks should be made out to the University of Wyoming and the department accepting payment - for example a purchase of athletic tickets should be made out to "University of Wyoming - Athletic Department."
- i. Checks should be restrictively endorsed with a stamp that has the following information-For Deposit Only- [department name] - [department number].
- j. Postdated or two-party checks should not be accepted for payment.
- k. Checks should only be accepted for the amount of the purchase (i.e. no cash back).
- l. Only United States currency and checks payable in U.S. dollars should be accepted. Checks drawn on foreign banks or issued in foreign currencies require special processing. Make note of them when preparing the deposit. The initial deposit will reflect the amount of the check, but exchange rate adjustments will be applied to the account after the check has been processed by the bank.

## **2. Reconciliation of collections and program activity**

- a. Funds must be counted daily and compared to receipt records.

- b. Permanent reconciliation records, including shortages or overages, must be prepared and retained. Overage and shortage activity should be closely monitored, as a measure of the effectiveness of the receipting process. Efforts should be made to identify the causes of such discrepancies and correct them.
- c. A continuous record of overages and shortages must be maintained and monitored. There is no acceptable level of discrepancy, but the cost of efforts to identify all causes and the cost of controls to ensure complete accuracy must be balanced against the potential for loss.
- d. Any theft or disappearance of funds must be immediately reported to Internal Audit and Campus Police for investigation. Risk Management should also be notified, although loss of funds may not be covered by insurance.
- e. Actual fund collections must be reconciled with the amount of revenue as reflected by the electronic receipting system, either at the close of business each day or as soon as possible following an event. This is usually accomplished with the use of a two-part form. One section contains an analysis of receipts used to calculate revenue amounts, and the other part contains a cash count. The totals developed in these two sections are compared, and the arithmetic difference shown as overage or shortage. If the department activity involves multiple sales or receipting points, a summary document is prepared to combine all activity into one statement.

### **3. Timely and intact deposits**

- a. Funds received must be deposited promptly and intact at the Cashiers Office or direct deposited into a University bank account if arrangements have been made with the Accounting Office.
- b. As soon as possible after reconciliation, collected funds should be transmitted to the appropriate office per Appendix D for credit to the appropriate University accounts.
- c. All deposits should be transported to the appropriate office per Appendix D in a locking bag. Information on obtaining locking bags can be requested from the Cashier's Office.
- d. All deposits must be made "intact"; that is, the amount deposited should relate exactly to a reconciliation document, which relates exactly to a group of receipts or receipt records from a specific period of time. Funds should be deposited in the order in which they are received, and in no case should funds be withheld for expenditure purposes.
- e. In the case of continual collection activities, deposits should be made

daily and within one working day of collection, whenever possible. If the department lacks secure facilities, efforts should be made to deliver funds to the Cashier's Office on the same day as collection. If collection activity is infrequent or small in amount, the cost of frequent transmittal should be balanced by the potential for loss. Departments are responsible for losses prior to transmittal to the Cashier's Office. The University Police Department and the Office of Risk Management can provide security guidance.

- f. If deposits are walked across campus to the Cashier's Office, two people should accompany the deposit for safety purposes. If the deposit contains a large amount of currency, an escort from the University Police Department can be requested.
- g. Departments shall not use campus mail to deliver deposits to the Cashier's Office
- h. The department should keep a record of the transmittal and Cashier's Office receipt for a minimum of seven years after the fiscal year in which the deposit is made for audit purposes.
- i. If control of the funds to be deposited is transferred from one department employee to another before deposit, a record of the amount transferred, signed by both employees, should be prepared and kept on file with the reconciliation and transmittal records.
- j. Approval to have funds direct deposited into a University bank account from the Payor must be obtained from the Accounting Office by emailing "[accounting-office@uwyo.edu](mailto:accounting-office@uwyo.edu)." The email must contain the Payor name and why funds are being collected. If approval is granted, the Accounting Office will supply the department with the necessary information to complete the transaction to provide to the Payor. It is the department's responsibility to communicate with the Payor. Once the Payor is set up and the department expects payment, the department should email "[uwaccts@uwyo.edu](mailto:uwaccts@uwyo.edu)" with Payor name, expected receipt amount, expected date of receipt, and chart string for posting to the financial management system each time a payment is anticipated. The Accounting Office will notify the department by email when the direct deposit funds are received.

#### **4. Financial records balancing**

- a. It is vitally important to reconcile departmental funds collection records with the University's general ledger accounting reports on a monthly basis.
- b. If transmittal, coding, and entry errors are made, only the collecting department can identify them. Receipt or transmittal records are

compared to account deposits and any differences must be identified.

- c. Departments must recognize timing differences such as accounting cut-off dates and times, and account for any in-transit deposits.
- d. Any discrepancy should be immediately brought to the attention of the Accounting Office, so that timely corrections can be made. If account balancing is done promptly each month, both the balancing process and corrections are much simpler.
- e. Whenever possible, the duties of receipt and deposit should be separated from account balancing. If only one employee is available for all tasks, the supervisor, or other appropriate designee, should review the records frequently, to ensure sufficient accountability.

## **5. Records retention**

After reconciliation and records balancing, records must be kept on file or stored in accordance with the [University of Wyoming Record Retention Schedules](#).

## **6. Training**

All employees who accept credit card payments or receive credit card information as part of their role at the University, must receive Payment Card Industry Compliance training at the start of employment and on an annual basis as long as they continue to accept credit cards or receive credit card information.

### **C. Acceptance Of Checks.** Because checks are generally not guaranteed cash items, additional steps need to be taken upon their receipt.

- 1. If a check is returned unpaid by a bank, it is essential that the Cashier's Office and Student Financial Services identify and communicate with the Payor. Before acceptance, department personnel receiving payment must view appropriate identification and verify that the check contains adequate Payor information, including full name, address, and telephone number, and that all information is current.
- 2. Checks should be made out to the University of Wyoming and the department accepting payment - for example a purchase of athletic tickets should be made out to "University of Wyoming - Athletic Department."
- 3. Checks should be restrictively endorsed with a stamp that has the following information - For Deposit Only - [department name] - [department number] immediately upon receipt.

4. Postdated, Third-Party, or Two-Party checks should not be accepted for payment.
5. Checks should only be accepted for the amount due or less than the amount due; they may not be accepted for more than the amount due (i.e. no cash back).
6. Only United States currency and checks payable in U.S. dollars should be accepted. Checks drawn on foreign banks or issued in foreign currencies require special processing. Make note of them when preparing the deposit. The initial deposit will reflect the amount of the check, but exchange rate adjustments will be applied to the account after the check has been processed by the bank.

**D. Acceptance of Credit/Debit Cards.** The University accepts credit/debit cards (payment cards) as payment for goods and services at retail operations around campus and as payment on student accounts for tuition, fees and other University charges. Transactions occur in person, over the telephone and via the internet. The University accepts Visa, MasterCard and Discover at all locations, and American Express at select locations. These are general processing guidelines for payment card acceptance. Each department may have additional processing guidelines specific to the systems and equipment in their location(s).

1. **General Operating Guidelines.** The following general guidelines are always applicable to payment card transactions:
  - a. **Do Not Set Restrictions on Card Transactions.** Discover, Visa and MasterCard prohibit setting a minimum or maximum purchase amount. University personnel are also prohibited from adding a surcharge to the transaction amount but may give a discount from the University's standard pricing for payment by cash.
  - b. **Protect Cardholder Privacy.** The University may only require a cardholder's personal information if it is necessary to complete a transaction or if the Voice Authorization Center specifically requests it. University personnel cannot refuse to complete a valid transaction just because the cardholder refuses to provide additional identification. Any additional information received to complete the transaction should not be written on the purchase receipt.
  - c. **Keep Cardholder Data Secure.** Receipts should only display the last four digits of a payment card number. Receipts should never contain the Payor's full payment card number. If there is a business need to write the Payor's card number or other sensitive authentication data, such as security codes, on paper, it should be stored in a locked area that is only accessible by select personnel. It should be stored in the locked area for

the minimum time necessary to complete the transaction and should be shredded immediately upon the transactions' authorization using a cross-cut shredder.

- d. Data Compromise.** Notify a supervisor and the UW Payment Card Industry Compliance Team, at [PCI@uwyo.edu](mailto:PCI@uwyo.edu), immediately if University personnel know or suspect that cardholder information has been accessed or used without authorization, even if this compromise involves a third-party vendor.

## **2. General Card Acceptance Procedures**

- a. Card Present Transactions.** Although there are different models of payment card acceptance machines around campus, the general steps to accepting a payment card payment are the same depending on the security features of the transaction card being presented. These steps include:

- i** Allow the customer to swipe a non-EMV card or dip an EMV card into the chip reader to begin the authorization process. If the EMV reader is not functioning correctly, the terminal will instruct the Payor to swipe the transaction card to complete the sale.
  - ii** Authorization is required for each transaction to determine if the card number is valid, the card has been reported lost or stolen, and that sufficient credit or funds are available to complete the transaction.
  - iii** One of the following responses will be received back from the authorization process:
    - 1.** Approval code;
    - 2.** Declined code (return card to Payor and request another form of payment);
    - 3.** Declined pick-up (do not return card to Payor); or
    - 4.** Referral/Call Authorization (call the Voice Authorization Center 1-800-741-5705 for further instructions).
  - iv** If an EMV card is presented, after receiving authorization, remind the Payor to remove the EMV card from the chip reader.
  - v** Obtain the cardholder's signature on the receipt.
  - vi** Compare the name, last 4 digits of the account number and the signature on the card to those on the receipt. If any of these items do



not match, make a Code 10 call as detailed in the Suspicious Activity section of this Policy.

**vii** Give a copy of the receipt to the Payor.

**viii** NEVER process an in-person sale without seeing the payment card. If someone wants to recite the payment card number from memory for you to process, stop the transaction and contact a supervisor.

Reduction in the risk of processing fraudulent payment card transactions occurs by processing Euro MasterCard Visa (EMV) chip enabled or non-EMV (Euro MasterCard Visa) transaction cards properly. Dual interface payment card terminals have been acquired by all campus merchants in order to process EMV transactions. Questions on Payment Card Industry (PCI) Compliance, assistance with a transaction card processing terminal or recent transaction batches should be directed through the to the UW Payment Card Industry Compliance Team at [PCI@uwyo.edu](mailto:PCI@uwyo.edu)

**b. Card Not Present Transactions.** Card Not Present Transactions include mail order, telephone order and electronic commerce transactions. These transactions occur when the card is not physically presented to the merchant at the time of sale. A TouchNet marketplace site is the UW PCI team's approved mode of collecting online payment. See the [TouchNet Marketplace Application](#) for more information.

**i** You must request permission to accept Card Not Present Transactions. Contact the UW Payment Card Industry Compliance Team at [PCI@uwyo.edu](mailto:PCI@uwyo.edu) to begin the approval process.

**ii** Card Not Present Transactions pose a higher risk of fraud and chargebacks, so it is important to take precautions when processing these transactions. Obtain the following information to process the payment:

1. Purchaser's name,
2. Cardholder billing address,
3. Shipping address, if different from billing address,
4. Cardholder's telephone number,
5. Cardholder's account number,
6. Card expiration date, and
7. CVV2/CVC2/CID number (3 digit code next to the signature

panel on the back of the card).

- iii After receiving the payment card information, process the transaction following the specific instructions for the Point of Sale system or device that you are using in your area. The cardholder's account number and CVV2 information can be maintained only to process the initial authorization and should be destroyed after that use. Do not store in hard copy or electronic format. Enter the CVV2 data directly into the terminal and do not write it down.
  - c. **Receipt.** A receipt for the transaction should be returned to the cardholder. If it is a mail order or telephone order, print the receipt, note the type of transaction on the signature line, and include the copy of the receipt with the invoice upon shipment of the item. For items paid through an e-commerce site, an electronic receipt of the transaction will be sent to the email address that was collected during the transaction.
3. **Fraud.** Be aware of the following possible signs of fraud. Contact a supervisor if you encounter any of these situations:
  - a. Request delivery to a freight forwarder.
  - b. Request to purchase items that the merchant does not sell (the most common items are laptop computer and cellular phones.)
  - c. Use of more than one card for a single transaction (also known as Split Ticket.)
  - d. Use of cards that have sequential numbers or patterns.
  - e. Utilize a phone relay service where the cardholder does not speak directly to the merchant.
  - f. Place an order and then call back to place subsequent orders using the same or different cards.
4. **Settling Transactions.** All payment card transactions should be settled daily and deposit information forwarded to the Accounting Office weekly. University personnel should follow the detailed instructions for the Point of Sale system or device being used for the settlement process and instructions from the Accounting Office for deposit information. Payment Card batch revenue should be recorded on a credit card revenue deposit advice form daily and deposited to the Accounting Office weekly.
5. **Reversing, Return or Exchange Payment Card Transactions.** When reversing a payment card transaction or accepting a return or exchange that was originally paid for with a payment card, the University must issue the credit transaction back to the original card used for payment. The customer

should be able to provide you with the original receipt and payment card to process the return. Do not refund a card purchase with cash or check. Do not refund cash or check purchases to a card.

6. **No Signature Required Transactions.** Certain categories of merchants can process transactions that do not require the signature of the cardholder. On the University campus, this type of transaction is limited to quick service food vendors. You must request permission to process no-signature transactions. Contact the UW Payment Card Industry Compliance Team, at [PCI@uwyo.edu](mailto:PCI@uwyo.edu), to begin the approval process. Approved vendors can process qualifying transactions with no signature from the customer and do not have to provide the customer a receipt unless they request it. The following criteria must be met:
  - a. Transaction amount is less than \$25.00.
  - b. The cardholder is present, and the transaction occurs in a face-to-face environment.
  - c. The full and unaltered content of the card's magnetic stripe is read and transmitted as part of the authorization; card must be swiped through a card reader; manual entry of the card number is not allowed.
  - d. One authorization is transmitted per clearing transaction.
  - e. The transaction is a domestic (U.S.) transaction.
  - f. Payment Card Security Features are present.
7. **Security Features.** It is recommended all University employees accepting payment card transactions become familiar with the security features of legitimate payment cards listed below. If a security feature is missing or appears to be tampered with, the individual processing the payment should contact a supervisor.
  - a. VISA cards should have a hologram of a dove on the front or the back of the card. Certain cards may also have a holographic magnetic stripe on the reverse side of the card. The VISA logo should be blue and gold on a white background, located in either the bottom right, top left or top right corner of the card.
  - b. MasterCard cards should have a hologram of two globes on the front of the card, above the MasterCard logo. Alternative card designs have the hologram on the back of the card and the MasterCard logo vertical in the upper right corner of the front of the card.
  - c. Card number, expiration date and cardholder name should be embossed, printed or laser etched on the card. All digits should be clear, in a

straight line, and be the same size/shape. Some vertical cards may have the numbers printed with four rows of four numbers.

- d. VISA card numbers should always start with a “4” and MasterCard card numbers should always start with a “5”.
- e. The signature panel on the back of the card has a tamper-evident design. If the panel has been erased and resigned, VOID may be displayed in the background of the panel.
- a. On VISA and MasterCard cards, the 3-digit CVV2 code should be printed in a white box just to the right of the signature panel. American Express cards have a 3-digit code on the back of the card, but it is rarely used. The number used to verify an American Express card is the 4-digit number found on the front of the card. Some cards will print the last four digits of the card number in the signature panel. Be sure that they match the front and the receipt and that they do not appear to be altered.

**8. Suspicious Activity.** In addition to following all of the standard payment card acceptance procedures, University personnel should also be aware of any Payor behavior that appears out of the ordinary. The following list, while not all inclusive, represents potential suspicious activity:

- a. Purchasing large amounts of merchandise with seemingly no concern for size, style, color or price.
- b. Trying to distract or rush the clerk during a transaction.
- c. Making purchases either right when the store opens or just before it closes.
- d. Questioning the sales clerk about credit limits or the authorization process.
- e. Signing the transaction receipt in a deliberate or unnatural manner.
- f. For card transactions that involve a card with “SEE ID” on the signature line, not having a driver's license or providing only a temporary license without a photo.
- g. Ships purchases to an address outside of the U.S.
- h. Recites the card number from memory rather than presenting the card itself.
- i. Asks to see the card again before signing the transaction receipt.

9. **Code 10 Call.** Peculiar behavior should never be automatically assumed to be fraudulent. University personnel will typically know what kind of behavior is normal for the specific place of business. If University personnel do encounter a transaction that is suspicious, the transaction should be reported by making a "Code 10" call. The term "Code 10" is used so the call can be made at any time during a transaction without arousing a customer's suspicions.
- a. Examples of specific situations where a Code 10 call would be in order include: card security features that are missing or irregular, or appear to have been tampered with; the last four digits of the account number on the receipt do not match the numbers embossed on the card; or University personnel receive a pick-up response when a card has been swiped for electronic authorization.
  - b. To make a Code 10 call, University personnel should keep the card in his or her possession during the call. Call the voice authorization center phone number (1-800-741-5705) and say, "I have a Code 10 authorization request." The call may be transferred to the University's acquiring bank, and University personnel will need to verify certain transaction details, but will ultimately be transferred to the card issuer and connected to a special operator. They will ask a series of questions that can be answered with a simple yes or no. When speaking to the special operator, answer the questions calmly and in a normal tone of voice. The answers will be used to determine if the card is valid. Follow all instructions given by the special operator. If the special operator tells University personnel to keep the card, do so only if retention or recovery is possible by reasonable and peaceful means. Never take unnecessary risks.
  - c. Upon successful retention or recovery of the card, the PCI Team should be called/ contacted immediately with a request for further instructions. Next, University personnel must cut the card in half lengthwise, being careful not to damage any holograms, the embossed account number, or the magnetic stripe, and then send the card pieces directly to PCI Team, who will return the card to the issuing bank.
  - d. If University personnel are not comfortable making a Code 10 call during a transaction or becomes suspicious of the transaction after the Payer has left, the call can still be made. A Code 10 call made after a transaction may help to stop future fraudulent card use at another retail location.
10. **Use Of Payment Device Connections to Transmit Payment Card Data**
- a. University personnel must always consult with the PCI Team before installing or making a change to a connection used by a payment device

to transmit payment card data.

- b. PCI Data Security Standards apply to all systems that store, transmit and process payment card data, including wireless Wi-Fi networks, wired and cellular networks, and analog phone connections.
- c. Point-to-point encryption (P2PE) solutions meet a higher standard of encryption. All PIN Transaction Security (PTS) certified devices encrypt data, but P2PE solutions use a different key to encrypt data for every transaction. P2PE validated solutions are common and merchants using properly implemented P2PE validated solutions as confirmed by the PCI team may use any type of connection: wired, wireless, cellular or analog phone because these solutions encrypt payment card data before transmission.
- d. Merchants using any other solutions for payment devices continue to be subject to restrictions and may not use wireless Wi-Fi networks. Cellular connections may be used if pre-approved by the PCI team chair. Unless a PCI chair approved solution such as Elavon' s SAFE-T injected terminal is used for wired network connections, merchants are required to use a specially configured restricted wired network to transmit payment card data.
- e. While analog phone connections approved by the PCI team are allowed, the alternate Elavon SAFE-T payment device solution is preferred when no P2PE Validated solution is in use.

#### **11. Important Phone Numbers**

- a. Voice Authorization Center:1-800-741-5705
- b. University Finance:1-307-766-3205

### **IV. ACCOUNTS RECEIVABLE**

Departments that provide goods and services on a charge and billing basis must keep accurate records of accounts receivable balances. These charges can be for anything that is receivable by a department including receivables from students or outside third parties. Such records should provide complete identification of purchaser, amount of sale, date of sale, billing activity, and payments. Funds collection records and receivable records should refer to each other. Charge records and billing invoices should also be pre-numbered, multi-copy documents. Billing of charge accounts should be done on at least a monthly basis.

Delinquent campus departmental accounts can be referred to the Student Financial Services Office for collection. Student Financial Services will facilitate collection of any funds due to the University, including student charges. Each department should define delinquency according to its collection history. The older a debt is, the less collectible it becomes. To maximize the possibility of full collection, it is strongly encouraged that outstanding accounts

be referred to the Student Financial Services when they are less than three months (90 days) old; however, the Student Financial Services accepts accounts that are older than ninety days. When referring a debt to the Student Financial Services Office, written documentation to support the original charge and copies of all invoices submitted to the account holder must be provided, as well as documentation of any email or phone contact that you have had in relation to collection of the debt.

The Student Financial Services Office determines when a debt should be referred to an outside collection agency and when a debt should be charged off as uncollectible. No other University departments can make a decision to charge off bad debt; they must refer the debt to the Student Financial Services Office. Successful collections by that office are paid to the referring department, and successful collections by outside agencies are paid to departments after deduction of the agency fee. Decisions about uncollectible items are communicated to the originating department for adjustment of receivables balances.

There is a significant cost to maintaining receivables. Departments should not allow credit or establish accounts receivable, unless there are compelling business reasons to do so, and adequate controls are in place. Departments must contact the Vice President for Budget and Finance if you feel there is a compelling business reason to allow credit or establish accounts receivable to gain approval before the credit or account is established.

**Responsible Division/Unit:** Division of Budget & Finance

**Links:** <http://www.uwyo.edu/regs-policies>

**Associated Regulations, Policies, and Forms:** UW SAP 7-9.13 Receipt and Handling of University Funds

**Approved:** 8/2/2022; 7/24/2025

## APPENDIX A- DEPARTMENTAL ROLES AND RESPONSIBILITIES

The following describes those departmental roles and responsibilities that relate to receipting and handling University funds.

- I. **Accounting Office:** The Accounting Office maintains the central University general ledger accounting system. The Accounting Office reconciles bank accounts, processes claims for working fund reimbursements, investigates errors identified by departments, and makes correcting entries when necessary.
- II. **Cashier's Office:** The Cashier's Office is responsible for receiving funds from departments, crediting them to the University's general ledger accounts, and depositing them in University bank accounts. In addition, the Cashier's Office issues instructions and provides training for the proper transmittal of funds, including issuing locked bags for transportation, and issues receipts for transmittals. The Cashier's Office balances cash receipts, properly allocates funds to bank accounts, and interfaces with banks and departments in the areas of deposit discrepancies and returned checks. The Cashier's Office also issues working fund advances for working (change) funds.
- III. **Departments:** All University departments (academic and administrative) that collect and receive funds in connection with departmental programs must have adequate systems and processes of control to guard against loss, ensure accountability, and provide an audit trail. These systems should be formalized in written policies and procedures and understood by all employees. A broad-based understanding is essential. Departments should not depend strictly on one or two key individuals.
- IV. **Employees:** It is the responsibility of all employees handling University funds to understand and comply with the provisions of this policy and departmental fund handling procedures. Employees must not engage in actions that risk loss or misuse of University assets.
- V. **Internal Auditor:** The Internal Auditor audits departmental financial records to verify the accuracy of records, adequacy of controls, and compliance with policies and procedures. The Internal Auditor verifies and audits working fund advances and recommends corrective action to appropriate officials. All losses must be reported to the Internal Auditor.
- VI. **Office of Risk Management:** The Office of Risk Management provides risk guidance and administers University insurance coverage. All losses must be reported to the Office of Risk Management.
- VII. **Officers:** It is the responsibility of all University officers to ensure that in their areas of responsibility, adequate internal controls exist to secure and account for all funds utilizing the University's cashiering and accounting systems. All officers must ensure that employees are aware of, understand, and are capable of complying with this policy.
- VIII. **Student Financial Services:** The Student Financial Services is responsible for the



collection of delinquent debts, collection of returned checks, and administration of the bad debt write-off policy for students and campus departments.

- IX. Supervisors:** Should have a thorough knowledge of the receipt and handling of University funds systems and processes in their areas of responsibility. They should regularly review employees' actions and records to verify that proper procedures are being performed and adequate internal control and accountability exists. Supervisors should be familiar with all University accounting reports pertinent to their areas.
- X. Tax Office:** The Tax Office performs the functions necessary for sales tax reporting and remittance to the State of Wyoming.
- XI. University Police:** University Police investigate and may charge individuals or entities in cases of forgery, theft, or criminal violations under Wyoming State statutes. All University losses must be reported to the University Police. In addition, the University Police conduct security surveys at departments' requests and can provide security guidance.
- XII. Vice President for Budget and Finance:** The Vice President for Budget and Finance is responsible for overseeing and implementation of the [Standard Administrative Policy and Procedure for Receipt and Handling of University Funds](#), this Financial Affairs Departmental Administrative Policy and Procedure for Receipt and Handling of University Funds, Payment Card Industry Compliance and provides administrative oversight to the University.

## **APPENDIX B - WORKING (CHANGE) FUNDS POLICY**

A working (or change) fund may be established if it can be demonstrated that a department needs cash on hand to make change during the process of a sales transaction.

### **I. PROCESS TO ESTABLISH A WORKING CASH FUND:**

- A.** The establishment of a working cash fund must be specifically approved by the Cashier's Office.
- B.** To request a working fund, submit a cash voucher form to the Cashier's Office with the signatures of the requestor, supervisor, and departmental cost center approver. If the Cashier's Office approves, the funds will be issued to the department. Once per month, the Cashiers Office will submit the cash vouchers to be recorded in the Financial Management System.
- C.** For both temporary (i.e., to make change at an event) and permanent working funds, fill out a cash voucher signed by the departmental authority and by the individual who will be collecting the cash. There should be two separate individuals signing.
- D.** The cash withdrawn by the department will be posted to 10-10008-000-000000-XXXXX-001-0000-0000-0. Note that natural account 10008-Cash Change Funds is an asset account and will not appear on account analysis reports that display only revenue and expenses. XXXXX represents the organization number. Make sure that this account code is provided in full.
- E.** If the amount requested is larger than \$2,500 or if specific denominations are required, contact the Cashiers Office in advance, either at 766-2313 or at [cashiers@uwyo.edu](mailto:cashiers@uwyo.edu), to verify that the cash is available.
- F.** The requestor listed on the cash voucher form must present a photo ID and the printed voucher to pick up funds from the Cashier's Office. A University ID is acceptable.
- G.** Cash Advance Voucher Forms are available at: [https://www.uwyo.edu/budget-finance/financial-affairs/\\_faffles/docs/fsbo/cashiers-office/cash-voucher-template.xlsx](https://www.uwyo.edu/budget-finance/financial-affairs/_faffles/docs/fsbo/cashiers-office/cash-voucher-template.xlsx).

### **II. PROCESS TO RETURN A WORKING CASH FUND:**

- A.** When the department no longer needs the working funds, the funds should be returned to the Cashier's Office and deposited into the same general ledger code on which the funds were drawn on (10-10008-000-000000-XXXXX-001-0000-0000-0.)
- B.** By taking out a working fund, the department agrees to the following:
  - 1.** To count, verify, and document the funds at the beginning of each day;

2. To reconcile and document the sales receipts of the working fund at the end of each day;
3. To keep the working fund amount in the department cash register/change box or safe; and
4. To only use the working fund to make change and never replenish from the Cashier's Office.

## **APPENDIX C - OTHER FINANCIAL POLICIES**

### **I. BUILDING/OFFICE KEY CHARGES**

- A.** Department heads and directors may require employees in possession of keys to University buildings and offices to pay for lost keys upon termination. Key charges may be assessed per the stated minimum and maximum amounts in the most recent copy of the University Fee Book and consistent with the [University Key Policies and Directives](#).
- B.** Key charges must be included on the terminated employee's termination form with the Payroll Office.

### **II. PERSONAL USE OF COPIERS AND OTHER OFFICE EQUIPMENT**

- A.** University computers, copy machines, fax machines and other office equipment are to be used for University business only. If departmental copy or fax machines are used for personal business of employees or students, departments should charge the established per copy rate. Established minimum and maximum rates can be found in the most recent copy of the University Fee Book. Funds collected for personal use of University equipment must be deposited, intact at the Cashier's Office.

### **III. ELECTRONIC PAYMENTS OUT OF A UNIVERSITY BANK ACCOUNT**

- A.** Automated Clearing House (ACH) payments may only be initiated by the University's Accounting Office using the bank's customer portal, which enhances the security of the transaction by the layered security features offered by these interfaces. Authorized signors will not initiate ACH payments in person at any bank branch except in limited cases. In those limited cases that an ACH would need to be initiated in-person at a bank branch, the Vice President for Budget and Finance or the Associate Vice President for Finance will accompany one of the authorized Accounting Office Personnel.
- B.** Wire transactions will only be initiated by authorized individuals within the Accounting Office by delivery of a letter which shall include wire details to the bank. Once in receipt of this letter, the bank will confirm the wire and amount with another authorized individual within the Accounting Office.
- C.** Wire transactions for investing purposes will only be initiated on the bank's customer portal by the authorized individuals within Financial Affairs to take advantage of the layered security features offered in these interfaces. In the case that the University's operating bank is not accessible due to technical difficulties, the steps required to initiate a wire transaction for operating purposes listed in the previous paragraph will be followed.
- D.** The overnight cash institution is only authorized to wire funds to the University's operating bank account. Wires out of the overnight cash institution are deposited directly into the general fund bank account. In the case the online customer portal

for overnight cash is not accessible due to technical difficulties, the Financial Affairs personnel may call the overnight cash institution to initiate the wire transaction into the general fund bank account.

- E.** The Accounting Office maintains a listing of recurring wires that occur either monthly or several times per year to increase control and monitoring of these transactions. These recurring wire transactions will only be initiated by the authorized individuals within the Accounting Office on the bank's customer portal, so that that enhanced layered security features offered by the interface are utilized. In the case that a recurring wire transaction would need to be initiated in-person at a bank branch, the Deputy Vice President for Budget and Finance or the Associate Vice President for Finance will accompany one of the authorized individuals within the Accounting Office.

## APPENDIX D

### DEPOSIT REMITTANCE LOCATION

The following table should be used to determine the remittance location for UW funds. Deposit type is based on the source of the funds.

Deposit type	Remit Checks / Receipts to:	How to Remit Deposits	Office Making the Deposit to UW's Bank
Deposit (cash and check) for payment of goods or services provided by a UW department or other funds that do not fall into the other categories in this table.	Cashier's Office Dept 3903 Knight Hall, Room 170	Refer to guidance at: <a href="https://www.uwyo.edu/fsbo/files/docs/cashiers/how-to-make-a-departmental-deposit.pdf">https://www.uwyo.edu/fsbo/files/docs/cashiers/how-to-make-a-departmental-deposit.pdf</a>	Cashier's Office
Scholarships	Office of Scholarships & Financial Aid Dept 3335 Knight Hall, Room 174	Deliver the check to the Office of Scholarships and Financial Aid.	When the Office of Scholarships and Financial Aid has processed the check, it will be routed to the UW Cashier's Office for recording in the general ledger and deposit to UW's bank account.
Funds to Reimburse UW for P-Card Violation	Procurement & Payment Services Dept 3605 Merica Hall, Rm 115	Deliver the check to the Procurement and Payment Services Office if you have been notified that a repayment to UW is required.	When the Office of Procurement & Payment Services has processed the check, it will be routed to the UW Cashier's Office for recording in the general ledger and deposited to UW's bank account.
Deposits related to ACH Funds or Credit Card Receipts	Accounting Office Dept 4330 Hill Hall, 5 <sup>th</sup> Floor North	Deliver the deposit to the Accounting Office	ACH: When the ACH has been received in UW's bank account, the Accounting Office will record it in the general ledger. Credit Card Receipts: The Accounting Office will reconcile the departmental credit card revenue deposit advice with the transactions that clear UW's bank and post the deposit in the general ledger
Award / Grant / Project related	Office of Sponsored Programs  Dept 4330 Hill Hall, Room 534, 5 <sup>th</sup> Floor South	1. Mail to OSP via campus mail attn: 2. Put the check in the drop box on the wall outside of the door of room 534 3. Deliver it to the front desk in room 534 Hill Hall	When the Office of Sponsored Programs has processed the check, it will be routed by the Office of Sponsored Programs directly to UW's bank account. Guidance can also be found on <a href="#">the Office of Sponsor Programs website</a> > FAQ's>Cash Management>How do I deposit a check?

**Gifts, Donations, and contributions should only be deposited at the UW Foundation, not at any of the locations in this table.**