



Department Administrative Policy and Procedure

Subject: Receipt and Handling of University Funds

Effective: 8/2/2022

PURPOSE

The policy and procedures, along with their attachments, are intended to assist University employees and others in the discharge of their fiscal responsibilities. The Policy and Procedures for Receipt and Handling of University Funds shall be administered by the Deputy Vice President for Budget and Finance or designee.

DEFINITIONS

Funds: Funds include currency, coin, checks, money orders, cryptocurrency and credit card transactions. Funds received on behalf of the University include, but are not limited to, departmental collections of revenue for programs and activities (including ticket sales), amounts collected as a result of the use of campus equipment and facilities, services provided by University employees, the on and off campus sales of goods, and services of University departments, and donations.

All funds of the University of Wyoming are public funds, 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.

Receipt and Deposit of Funds. The Policy and Procedures for Receipt and Handling of University Funds and attachments set forth details for receipt and deposit of University funds. However, the following highlight some general requirements relating to receipt and deposit of University funds.

- a. All funds received on behalf of the University must be acknowledged by receipt when received and deposited intact in the Cashier's Office, Knight Hall, Room 170.
- b. Deposits are intact when 100 percent of the funds received are deposited, no funds are withheld from the deposit, and contemporaneous written receipts are prepared documenting the funds received.
- c. **Individual departments and programs may not establish a bank account, or otherwise withhold University funds from deposit to official University accounts.**
- d. All receipts collected by departmental personnel in the performance of assigned duties are considered public funds and must be deposited with the Cashier's Office.
- e. Donations, contributions and gifts to the University are properly deposited to and retained by the University of Wyoming Foundation. Foundation financial personnel should be consulted in the event a gift is received directly by a campus department.

POLICY

This policy is not intended to be all-inclusive; inevitably, there are situations not specifically addressed here. It is intended that the basic principles discussed will provide procedures applicable to most situations. Additional assistance is available from UW Financial Affairs offices: specifically the Associate Vice President of Finance Office and the Cashier's and Accounting Offices. Risk Management, Internal Audit and/or University Police can also provide valuable information as needed.

The main objectives of the receipt and handling of University funds policies, procedures and controls are to guard against loss and ensure accountability. University systems are designed to control the receipt, deposit, and expenditure of all funds, and to account for them properly.

All departments that handle funds must develop departmental funds handling procedures that comply with the campus policy, including but not limited to the following procedures:

- Duties of opening mail, processing funds received by mail, collecting cash, preparing receipts and account reconciliation should be separated among individuals (i.e. one individual is not responsible for two or more of these activities) to the extent allowed by staffing resources.
- Departmental funds handlers must take periodic vacations, during which time another employee performs funds handling duties.
- Any theft or disappearance of funds should be immediately reported to Internal Audit and Campus Police for investigation. Risk Management and Insurance should also be notified, although loss of funds is generally not covered by insurance.

Basic Elements of Receipt and Handling of University Funds

The basic elements of receipt and handling of University funds are explained in detail below:

- a. Receipt processes and documents
 - b. Reconciliation of collections and program activity
 - c. Timely and intact deposits
 - d. Financial records balancing and
 - e. Record retention
- a. Receipt processes and documents

Receipt records must be prepared at the time funds are received into a University bank account in order to provide revenue accounting and

reconciliation with actual funds collected.

- i. Revenue records are also necessary for program management and tax reporting purposes.
- ii. Multi-copy receipting systems such as electronic cash register receipts or pre- numbered hand written receipts are acceptable forms of receipt documents.
- iii. The payer should be given the original pre-numbered receipt if a receipt book is used. The carbon copy should be left in the book.
- iv. For retail sales, cash register receipts should be given to the payer.
- v. For ticket sales, the pre-numbered ticket given to the payer is the receipt and no other receipt is necessary.
- vi. For concessions or vending sales, receipts are not required.
- vii. Direct deposits to university bank accounts are exempt from the receipt requirement.
- viii. 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 UW - Athletic Department.
- ix. Checks should be restrictively endorsed with a stamp that has the following information-For Deposit Only- [department name] - [department number].
- x. Postdated or two-party checks should not be accepted for payment.
- xi. Checks should only be accepted for the amount of the purchase (i.e. no cash back).
- xii. 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.

b. Reconciliation of collections and program activity

Cash, checks, money orders and credit card transactions must be counted on a daily basis and compared to receipt records.

- i. 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.
- ii. 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.

- iii. Any theft or disappearance of funds should be immediately reported to Internal Audit and Campus Police for investigation. Risk Management and Insurance should also be notified, although loss of funds is generally not covered by insurance.
 - iv. Actual fund collections must be reconciled with the amount of revenue as reflected by the 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.
- c. Timely and intact deposits

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.

- i. As soon as possible after reconciliation, collected funds should be transmitted to the Cashier's Office for credit to the appropriate University accounts.
- ii. All deposits should be transported to the Cashier's Office in a locking bag. Information on obtaining locking bags can be requested from the Cashier's Office.
- iii. 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.
- iv. 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.
- v. 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.
- vi. Departments shall not use campus mail to deliver deposits to the Cashier's

Office

- vii. The department should keep a record of the transmittal and Cashier's Office receipt for three years after the fiscal year in which the deposit is made for audit purposes.
 - viii. 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.
 - ix. Approval to have funds direct deposited into a university bank account from the customer must be obtained by the UW department emailing accounting-office@uwyo.edu. Please provide the customer 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 customer. It is the department's responsibility to communicate with the customer. Once the customer is setup and the department expects payment, the department should email accounting-office@uwyo.edu with customer 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.
- d. Financial records balancing
- It is vitally important to reconcile departmental funds collection records with the University's general ledger accounting reports on a monthly basis.
- x. 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.
 - xi. Departments must recognize timing differences such as accounting cut-off dates and times, and account for any in-transit deposits.
 - xii. 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.
 - xiii. 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 should review the records frequently, to ensure sufficient accountability.

e. Records retention

After reconciliation and records balancing, records must be kept on file or stored in accordance with the following University of Wyoming Record

Retention schedules found at: <https://www.uwyo.edu/ahc/uw-archives/schedules.html>.

ACCEPTANCE OF CHECKS

Because checks are generally not guaranteed cash items, additional steps need to be taken upon their receipt.

If a check is returned unpaid by a bank, it is essential that the Cashier's and Accounts Receivable Offices 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. Verify that all information is current.

- 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 UW - Athletic Department.
- Checks should be restrictively endorsed with a stamp that has the following information - For Deposit Only - [department name] - [department number].
- Postdated or two-party checks should not be accepted for payment.
- Checks should only be accepted for the amount of the purchase (i.e. no cash back).
- 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.

- ACCEPTANCE OF CREDIT/DEBIT CARDS

The University of Wyoming 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. Your department may have additional processing guidelines specific to the systems and equipment in use at your location(s).

General Operating Guidelines

The following general guidelines are always applicable to payment card transactions:

1. 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.
2. 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.
3. Keep Cardholder Data Secure: Receipts should only display the last four digits of a payment card number. Receipts should never contain the customer's full payment card number. If there is a business need to write the customer 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.

Data Compromise: Notify a supervisor and the UW Payment Card Industry Compliance Team at 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.

General Card Acceptance Procedures

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. You will be assisting the University in reducing the risk of processing fraudulent payment card transactions 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 have the ability 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.

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 customer to swipe the transaction card to complete the sale.

- a. 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.
- b. One of the following responses will be received back from the authorization process:
 - i. Approval code;
 - ii. declined code (return card to customer and request another form of payment);
 - iii. declined pick-up (do not return card to customer), or
 - iv. Referral/Call Authorization (call the Voice Authorization Center 1-800-741-5705 for further instructions).
- c. If an EMV card is presented, after receiving authorization, remind the customer to remove the EMV card from the chip reader.
- d. Obtain the cardholder's signature on the receipt.
- e. Compare the name, last 4 digits of the account number and the signature on the card to those on the receipt.
 - i. If any of these items do not match, make a Code 10 call as detailed in the Suspicious Activity section below of this policy.
- f. Give a copy of the receipt to the customer.

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.

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 site application at: http://www.uwyo.edu/fsbo/_files/docs/co-touchnet-marketplace-application.pdf

You must request permission to accept Card Not Present transactions. Contact the UW Payment Card Industry Compliance Team at PCI@uwyo.edu to begin the approval process.

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:

- Purchaser's name

- Cardholder billing address
- Shipping address, if different from billing address
- Cardholder's telephone number
- Cardholder's account number
- Card expiration date
- CVV2/CVC2/CID number (3 digit code next to the signature panel on the back of the card)

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. Please note that 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.

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.

Be aware of the following possible signs of fraud. Contact a supervisor if you encounter any of these situations:

- Request delivery to a freight forwarder.
- Request to purchase items that the merchant does not sell (the most common items are laptop computer and cellular phones).
- Use of more than one card for a single transaction (also known as Split Ticket).
- Use of cards that have sequential numbers or patterns.
- Utilize a phone relay service where the cardholder does not speak directly to the merchant.
- Place an order and then call back to place subsequent orders using the same or different cards.

Settling Transactions

All payment card transactions should be settled daily and deposit information forwarded to the Cashier's office. Follow the detailed instructions for the Point of Sale system or device that you are using for the settlement process and instructions from the Cashier's office for deposit information. Payment Card batch deposits to the Cashier's office should be conducted daily and may be emailed to the Cashier's Office at Cashiers@uwyo.edu. A receipt for this deposit will be sent to you via campus mail.

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.

No Signature Required Transactions

Certain categories of merchants can process transactions that do not require the signature of the cardholder. On the UW 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 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:

1. Transaction amount is less than \$25.00.
2. The cardholder is present and the transaction occurs in a face-to-face environment.
3. 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.
4. One authorization is transmitted per clearing transaction.
5. Applies to domestic (U.S.) transactions only.

Payment Card Security Features

It is recommended you become familiar with the security features of legitimate payment cards listed below. If you notice a security feature is missing or appears to be tampered with, please contact a supervisor.

- c. 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.
- d. 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.
- e. 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 (4) rows of four (4) numbers.
- f. VISA card numbers should always start with a 4 and MasterCard card numbers should always start with a 5.
- g. 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.

- h. 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 four digit number found on the front of the card. Some cards will print the last 4 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.

Suspicious activity

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

- Purchasing large amounts of merchandise with seemingly no concern for size, style, color or price.
- Trying to distract or rush the clerk during a transaction.
- Making purchases either right when the store opens or just before it closes.
- Questions the sales clerk about credit limits or the Authorization process.
- Signs the transaction receipt in a deliberate or unnatural manner.
- Does not have a driver's license or provides only a temporary license without a photo - applicable only to card transactions that involve a card that says SEE ID on the signature line.
- Ships purchases to an address outside of the U.S.
- Recites the card number from memory rather than presenting the card itself.
- Asks to see the card again before signing the transaction receipt.

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. 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 UW'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 recovery is possible by reasonable and peaceful means.

If University personnel are not comfortable making a Code 10 call during a transaction or becomes suspicious of the transaction after the customer has left the store, 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.

The following are some specific situations where a Code 10 call would be in order:

- Card security features are missing or irregular, or appear to have been tampered with.

The last 4 digits of the account number on the receipt do not match the numbers embossed on the front of the card.

University personnel receive a pick-up response when a card has been swiped for electronic authorization.

If University personnel are asked by an operator to recover a suspicious card, remember the following guidelines:

- Recover the card only if it can be done safely. Never take unnecessary risks.
- Tell the cardholder you have been instructed to keep the card and that he or she may call the card issuer for more information.
- Remain calm and courteous. If the cardholder behaves in a threatening manner, return the card immediately.
- If you successfully recover the card, immediately call the Treasury Management and Financial Services office and ask for further instructions.
- Cut the card in half lengthwise, being careful not to damage any holograms, the embossed account number, or the magnetic stripe.
- Send the card pieces directly to the Treasury Management and Financial Services office, who will return the card to the issuing bank.

Use of payment device connections to transmit payment card data

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.

The Payment Card Industry (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.

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.

Point to Point Encrypted (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.

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.

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.

Important Phone Numbers

- Voice Authorization Center:1-800-741-5705
- Finance:1-307-766-3205

ACCOUNTS RECEIVABLE

Departments that provide goods and services on a charge and billing basis must keep accurate records of accounts receivable balances. 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. 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 Accounts Receivable Office when they are less than three months (90 days) old, however the Accounts Receivable Office accepts accounts that are older than 90 days. . When referring a debt to the Accounts Receivable Office, please be sure that you have written documentation to support the original charge and copies of all invoices submitted to the account holder, as well as documentation of any email or phone contact that you have had in relation to collection of the debt.

The Accounts Receivable 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 Accounts Receivable 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. Please contact the Deputy 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.

APPENDIX A- DEPARTMENTAL ROLES AND RESPONSIBILITIES

The following discussion concerns only those departmental responsibilities that relate to receiving and handling University funds. It is not meant to be an in-depth description of employee or departmental functions.

A. Employees: It is the responsibility of all employees handling University funds to understand and comply with the provisions of this policy. Employees must not engage in actions that risk loss or misuse of University assets.

B. 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.

C. 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 cashing and accounting systems. All officers must ensure that employees are aware of, understand, and are capable of complying with this policy.

D. 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.

E. 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 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.

F. 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.

G. 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.

H. Tax Office: The Tax Office performs the functions necessary for sales tax reporting and remittance to the State of Wyoming.

I. Deputy Vice President for Budget and Finance: The Deputy Vice President for Budget and Finance is responsible for the Receipt and Handling of University Funds Policy and Procedures and Payment Card Industry Compliance and provides administrative oversight.

J. Risk Management and Safety: The Office of Risk Management and Safety provides security guidance and administers University insurance coverage. All losses must be reported to the Office of Risk Management.

K. 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.

L. University Police: University Police investigate and may prosecute in cases of forgery, theft, or criminal violations under Wyoming State statutes. All losses must be reported to the University Police. In addition, the Police conduct security surveys at a department's request, and can provide security guidance.

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.

Process to establish a working cash fund:

The establishment of a working cash fund must be specifically approved by the Cashier's Office.

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 will submit the cash vouchers to be recorded in the Financial Management System.

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.

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.

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 to verify that the cash is available.

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. University ID is acceptable.

Cash Advance Voucher Forms are available at https://www.uwyo.edu/fsbo/_files/docs/cash-voucher-template.xlsx .

Process to return a working cash fund:

When the department no longer needs the working funds the funds should be deposited at the cashier's office back to the same general ledger code that the funds were drawn on 10-10008-000-000000-XXXXX-001-0000-0000-0.

By taking out a working fund, the department agrees to the following:

- To count, verify and document the funds at the beginning of each day
- At the end of each day the working fund should be reconciled to sales receipts and documented.
- The working fund amount is kept in the department cash register/change box or safe.

A working fund should never need to be replenished by the Cashier's Office, as its only purpose is to make change.

APPENDIX C - OTHER FINANCIAL POLICIES

Building/Office Key Charges

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.

Key charges must be included on the terminated employee's termination form with the Payroll Office.

Personal Use of Copiers and Other Office Equipment

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. <https://www.uwyo.edu/administration/financial-affairs/feebook/>. Funds collected for personal use of University equipment must be deposited intact at the Cashier's Office.

Electronic Payments Out of a University Bank Account

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 Deputy Vice President for Budget and Finance or the Associate Vice President for Finance will accompany one of the authorized Accounting Office Personnel.

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.

Wire transactions for investing purposes will only be initiated by the authorized individuals within Financial Affairs on the bank's customer portal to take advantage of the layered security features offered in these interfaces. In the case that UW'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.

The overnight cash institution is only authorized to wire funds to UW'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.

The University of Wyoming 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.

Responsible Division/Unit: Budget and Finance Division

Links:

Associated Regulations, Policies, and Forms: [Receipt and Handling of University Funds Standard Administrative Policy and Procedure \(SAPP\)](#)