

**BOARD OF COUNTY COMMISSIONERS
COUNTY OF KITTITAS
STATE OF WASHINGTON**

RESOLUTION NO. 2024- 013

A RESOLUTION ADOPTING THE KITTITAS COUNTY CASH HANDLING MANUAL

WHEREAS, the Board of County Commissioners adopted the Cash Handling Policy and Procedures on November 5, 2019; and

WHEREAS, the Washington State Auditor's office recommends that counties have cash, cash receipting, credit card, banking, and EFT policies and procedures approved and implemented to provide for the continued safety of public monies;

WHEREAS, the current policy has been updated to reflect updated RCWs, SAO guidance, county best practices, current changes to banking, and software changes;

NOW THEREFORE, BE IT RESOLVED: WHEREAS, these policies may be changed from time to time, and should not take the form of a resolution; and WHEREAS, any and all deletions, additions, or changes to current policies will require a new resolution to adopt the new Table of Contents with those changes;

NOW, THEREFORE, BE IT RESOLVED that the "Cash Handling Manual" has been adopted with the attached Table of Contents.

NOW, THEREFORE, BE IT RESOLVED: Resolutions No. 2011-002, 1999-62, and 1999-99 are hereby rescinded in their entirety and replaced Resolution 2024- 013 Kittitas County Cash Handling Manual.

Dated this 18th day of January 2024, at Ellensburg, Washington.




☒ Clerk of the Board – Julie Kjorsvik

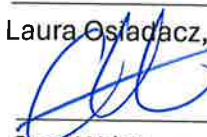
☐ Deputy Clerk of the Board – Mandy Buchholz



BOARD OF COUNTY COMMISSIONERS
KITTITAS COUNTY, WASHINGTON


Brett Wachsmith, Chairman
ABSENT

Laura Osladacz, Vice-Chairman


Cory Wright, Commissioner

75-268A



Policy and Procedures Manual for Cash Management



Table of Contents

CHAPTER 1:

Cash Handling Policy and Procedures.....	1
Purpose	1
Authority	1
Policy and Procedures	1
Custodial Responsibility and Liability	1
Cash Handler Training	2
Cash Handling Compliance	2
Cash Handling	3
Definitions	3
Handling Cash	3
Acceptance of coins.....	4
Balancing A Cash Drawer.....	4
Large Cash Transactions	4
Cash Drop	5
Cash Overages and Shortages	5
Recurring Offages	6
Checking for Counterfeit Bills	7
Altered Currency	7
Cash Receipting.....	9
Deposits.....	9
Tendering Checks, Check-like items (warrants, money orders, etc.), and Credit/Debit Cards.	9
Receipting.....	10
Receipting "over-the-counter" payments	11
Receipting Payments by Mail	11
Internal Controls.....	12
Deposits	14
Preparing Deposits	14
Reporting of Losses.....	16
Petty Cash	18
Bank Returned (NSF) Checks.....	20
Non-County Money	21
Monetary Gifts	21
Donation.....	21
Found Property.....	21
Non-County Funds.....	21
Daily Pickup of County Funds for Bank Deposit.....	22
Deposits.....	22
Safeguarding Funds in an Emergency	24
Robbery	24
Fire or natural disaster	25

CHAPTER 2:

Credit Card Policy and Procedures	26
Purpose	26
Summary Statement.....	26
Acceptable Credit or Debit Cards	26
Prohibited Credit or Debit Card Activities	26
Credit or Debit Card Fees	27

Refunds.....	27
Chargebacks	27
Maintaining Security	27
Wireless Technology	28
Sanctions	28
Training.....	28
Processing Procedures	29
Department Responsibilities	29
Treasurer Responsibilities	30
Information Technology Responsibilities	30

CHAPTER 3:

EFT Policy and Procedures	31
Background.....	31
Statement.....	31
Processes and Instructions	31
ACH Processing.....	31
Domestic External Wires	32
International External Wires	32
Book Transfers.....	33
Treasurer's Banking Information Requests	33
Fraud Protection and Safeguard Procedures	33

APPENDIX

Appendix 1: Recognizing Currency and Coin.....	34
Appendix 2: How to Control Cash in a Small Office	36
Appendix 3: Reporting a Loss	38
Appendix 4: PCI Compliance Monitoring Process for Kittitas County.....	39
Appendix 5: Glossary.....	41
Appendix 6: Internal Controls Checklist.....	44
Appendix 7: Acknowledgment Form – Cash Management.....	50
Appendix 8: Credit Card Policy Acknowledgment Form	51

CHAPTER 1:

Cash Handling Policy and Procedures

Purpose

The purpose of the " Kittitas County Cash Handling Policy and Procedures" is to create a guideline for all Kittitas County employees who bear the responsibility for the collection and handling of cash as part of their job responsibilities. The goal of this manual is to provide the tools to minimize risk and losses, increase awareness of responsibility, and ensure compliance with the RCW and State Auditor's requirements.

Authority

Washington State Constitution Article XI, 15, and Revised Code of Washington (RCW) 36.29.010, describe the general duties of the County Treasurer as it pertains to cash handling as follows:

- 1) Shall receive all money due to the county and disburse it on warrants issued and attested by the County Auditor.
- 2) Shall issue a receipt in duplicate for all money received other than taxes; the treasurer shall deliver immediately to the person making the payment the original receipt and the duplicate shall be retained by the treasurer.
- 3) Shall maintain financial records reflecting receipts and disbursements by fund in accordance with generally accepted accounting principles.

Policy and Procedures

Many of the cash handling duties and responsibilities assigned to the County Treasurer by law include actions by other County officers, employees, and agents. To ensure that all County employees responsible for handling cash are aware of their responsibilities, the following policies and procedures will provide rules and guidelines for all cash handlers in Kittitas County. In the event of a conflict between these policies and procedures and those adopted by a department, these policies and procedures shall take precedence.

Departments are expected to keep employees who handle cash informed of all County cash handling policies and procedures. All employees who are involved in the handling of monies are expected to be accurate and efficient when processing customer payments, making change, or accepting checks. They are also expected to safeguard County funds against loss and to establish and maintain good customer relations. All existing and future employees who handle cash are required to verify that they have read and accepted the Kittitas County Cash Handling Policy and agree that any violation of said Policy may result in disciplinary action up to and including termination and possible criminal prosecution.

Custodial Responsibility and Liability

A custodian is personally responsible for all County money within his/her control and may be held liable for any loss occurring unless an act of God, a robbery, or a statutory exception caused the loss.

- 1) All County cash handlers shall comply with their departments and the Kittitas County Cash Handling Policies. All cash handlers who fail to comply with their departments or the Kittitas County Cash Handling Policies may be subject to disciplinary action, up to and including termination.
- 2) All cash handlers who obtain custody of County money are personally responsible until the money is deposited with one of the County Treasurer's authorized agents or banks, and may be held liable for any loss, theft, or statutory exception.
- 3) It is strongly encouraged that all cash handlers employed by Kittitas County must complete a background check.
- 4) All transfers of custody of County money to the Kittitas County Treasurer shall be documented on a Cash Suspense Receipt approved by the Kittitas County Treasurer and must include the specifications of the breakdown of cash, checks, electronic transfers, and remote deposits, the department for whom the deposit is being made, and the name of the person who completed the Cash Suspense Receipt on behalf of the department.
- 5) Any department cashier who issues a written receipt accepting custody of County money is responsible and liable for the timely deposit of that money. The liability for timely deposit starts with the original receipt of County money by a County officer, employee, or agent and ends when the money is deposited with the County Treasurer or bank. All money received must be deposited within 24-hours unless authorization to waive the 24-hour deposit requirement has been approved by the Treasurer. Under no circumstances shall funds be held for more than one week.
- 6) Temporary employees hired by a county department may be utilized as a cash handler must follow the same procedures outlined throughout this manual.

Cash Handler Training

All County employees involved with the handling, receipting, reconciling, or depositing of money shall read and understand the Kittitas County Cash Handling Policy and Procedures. It shall be the responsibility of the Department Head, Elected Official, or designee of each department to ensure each cash handler's compliance.

- 1) Any employee determined to have cash handling duties or responsibility shall read the Cash Handling Policy and Procedures within 30-days of hire or assignment of duties.
- 2) For special events Kittitas County may contract temporary cash handlers. Kittitas County may assign the Treasurer's lead cashier to train the temporary employee. If the employment period is anticipated to be 30-days or longer, the contracted employee must read and understand the Policy.

Cash Handling Compliance

- 1) It is the responsibility of each Elected Official/Department Head to provide training to all employees involved in handling, receipting, reconciling, and depositing money, to ensure compliance with the requirements of the Kittitas County Treasurer.
- 2) The Kittitas County Treasurer shall provide any clarification of the Kittitas County Cash Handling Policy and Procedures.
- 3) The Elected Official/Department Head shall allow the Kittitas County Treasurer or his/her authorized deputy to periodically inspect and report on the department's cash handling procedures.
- 4) The Elected Official/Department Head shall designate a department cashier to handle the transmittal of funds and deposits to the Kittitas County Treasurer.

Cash Handling

Description

Consistent use of Best Practices is a key element to our success. This procedure outlines good cash handling, organization of tills, proper handling of checks, cash, and other forms of payment, source documents that need to be saved, and how to check for counterfeit currency.

Processes & Instructions

Definitions

- *Cash Drawer (aka 'Till')*: The till where you place your starting cash.
- *Fraud Fighter*: A device that detects counterfeit bills.
- *Flashlight*: A small flashlight with UV Black Light used to detect counterfeit bills
- *Jog/Jogged*: Aligning paper or notes together to form a neat stack.
- *Cash Drop*: Removing and safeguarding excess funds when the till contains \$10,000 or currency is overflowing even though the till is not at \$10,000.
- *Dual Custody*: Two team members (Cashier and Manager or Lead) transporting, counting, and securing currency.

Handling Cash

- 1) Each cash drawer contains coins and currency which should be arranged in a consistent manner.
- 2) Only currency and coins may be stored in a cashier's till at the Front Counter.
 - a. Under no circumstances should jewelry, lunch money, make-up, candy, or other personal items be found in a cash drawer or any other location where checks or currency are kept.
- 3) Always ensure the cash and cash drawer are secured.
 - a. Drawers at the front counter are to remain locked unless needed during a transaction, checks are to be placed in the cashier's drawer in the order they were receipted.
- 4) Cash drawers, prepared deposits, and/or till keys are not to be left unattended while in the back office or front counter.
- 5) Keys to a station's drawer are not to be left in the keyhole.
 - a. Keys should be restricted to the minimum possible number of employees. A written record of office keys should be maintained, and it is the responsibility of a terminated or transferred employee's supervisor to ensure that keys are returned by terminated or transferred employees. If combination locks are used, the combination should be changed annually or whenever an employee who knows the combination terminates County employment or transfers to another department.
- 6) Follow Best Practices for Checking for Counterfeit Bills.
- 7) Cash is to be counted a minimum of twice when being receipted; up to as many times as it takes to get the same amount twice.
 - a. Before counting separate and face currency and coin by denominations.
- 8) If change is required, both coin and currency are to be counted a minimum of two times to confirm it is correct; then counted a third time out loud to the customer when giving them their change.

- 9) Tender currency/coin received; enter the amount the customer is tendering to reflect cash returned to the customer.
 - a. Example: Transaction totaling \$1,455.00; customer pays \$1,500.00 in currency; enter \$1,500.00 and the point of sale will calculate the amount of change due to the customer.

Acceptance of coins

- 1) The United States Department of Treasury has determined that although coins are legal tender under the Coinage Act of 1965, no Federal statute mandates acceptance of coins for payment, and because no Washington state law mandates such acceptance for payment, the County has adopted a coin acceptance policy on payments to promote office efficiencies and the timely provision of services to its residents.
- 2) Acceptance of coins for payments of fines, debts, taxes, and other public obligations may be refused under the following circumstances:
 - a. When the coins are bent, broken, damaged, or delivered in unsanitary conditions.
 - b. When the coins are non-U.S. coins.
 - c. When coins exceed \$20 in amount.
- 3) Coin must be delivered in rolled sleeves with a receipt designating the amount being delivered if the number of coins exceeds standard banking procedure (see Appendix 1.) For example: 51 dimes would require a roll of 50 plus one loose dime.
- 4) The payor will be responsible for all identified shortages upon a coinage count and payment validation by the bank.

Balancing A Cash Drawer

Persons who collect County money from the public shall balance their cash drawer daily. All money should be balanced and deposited with the County Treasurer according to RCW 43.09.240, which states in part... "Every public officer and employee, whose duty it is to collect or receive payments due or for the use of the public, shall deposit such money collected or received by him or her with the treasurer of the taxing district every twenty-four consecutive hours. The treasurer may in his or her discretion grant an exception where such daily transfers would not be administratively practical or feasible."...

Cash drawers will be balanced to receipts daily, and Elected Officials/Department Heads are to designate an employee to handle the transmittal of funds and deposits to the Treasurer's Office.

For balancing a cash drawer, the following procedure is recommended:

- 1) All currency and coin is counted and listed by denomination on a cash count sheet.
- 2) The cash handler lists all checks on an adding machine tape, or an Excel spreadsheet, and transfers the check amount to the cash count sheet. The cashier should confirm that all checks have the required endorsement stamp.
- 3) Total all of the receipts written.
- 4) The total of cash and checks should be equal to the total receipts written, less the beginning cash drawer balance.

Large Cash Transactions

When receiving cash for a tax payment, bail money, or deposit, regardless of the amount, all the following steps must be adhered to:

- 1) Determine the amount of cash being received.
- 2) If the cash is \$5,000.00* or more, dual custody is required when counting. Request that a co-worker witness you counting the cash. You may also request that the co-worker count the cash.
 - a. If the cash is less than \$5,000.00, dual custody is not required, under this policy, but the cash handler must request dual custody.
- 3) Do not place the cash in your drawer until the amount has been verified and receipted.
- 4) Do not leave the cash unattended.
- 5) On the receipt, confirm the amounts posted and any cash back.
- 6) Give the receipt to the customer.
- 7) Print a receipt for yourself and wrap it around the cash with a rubber band.

Cash bail over \$10,000 in two or more related transactions received by a court clerk or anybody receiving bail on the clerk's behalf, presumably a sheriff's office is required to file IRS Form 8300.

**minimum threshold*

Cash Drop

Cashiers should maintain an awareness of how much cash has passed through their till. When the drawer balance exceeds the amount set by policy, or the number of bills makes it physically difficult to deal with, funds should be removed from the drawer and secured to safeguard the cash from loss or theft. This should be done using the steps outlined below:

- 1) When a cashier's till reaches \$10,000 or there is no room for additional cash a cash drop will be completed.
- 2) The cash drawer is counted back down to its original starting amount, and the remainder of the money is removed to a secure location.
- 3) The cash drop should be made in dual control with the cashier and a member of management.
- 4) The cashier removes large denomination bills and counts the cash using a ten-key calculator which will be initialed and dated by the cashier and manager.
- 5) The cash will then be secured in a sealed bank bag and placed in the cashier's locking drawer in the department/office vault.
- 6) **Reminder:** Retrieve the dropped amount secured in the cubby or drawer before balancing.

Cash Overages and Shortages

All funds received by County employees are to be deposited intact (as received) to the Treasurer's Office.

In the event of a suspected loss of public funds, the correct procedures must be followed to minimize the loss. If a loss occurs the following procedures should be followed:

RCW 43.09.185 requires that all state agencies and local governments **immediately** notify the State Auditor's Office (SAO) in the event of a known or suspected loss of public funds or assets or other illegal activity. *See reporting of losses pg. 15

This guidance should establish an individual responsible for informing managers and employees about these reporting requirements and ensuring the SAO is promptly informed of losses as required. These actions will also help to ensure that:

- Losses are minimized.
- Investigations and audits are not hampered.
- Improper settlements are not made with employees.
- Incorrect personnel actions are not taken.
- Employees are protected from false accusations.
- Bond claims are not jeopardized.

If, upon balancing daily receipts, it is discovered that the funds to be deposited do not equal the receipt posted, an over/short situation exists per Resolution 2023-074. If, after an appropriate search for any missing funds and/or recalculation of funds to be deposited and receipts posted, the over/short situation remains, complete the following procedures:

- 1) Complete the "Cash Suspense Receipt" as documented by the receipts.
 - a. The Cash Suspense Receipt must be submitted identifying the composition of checks and cash collected and deposited by the cash handler. To ensure that the monies are recorded correctly, the completed Cash Suspense Receipt must include the following information:
 - i. Amount of the deposit.
 - ii. Date
 - iii. Name of the department depositing.
 - iv. Fund # that the revenue is to be credited to.
 - v. Appropriate BARS number identifying the source of the revenue.
- 2) If the funds to be deposited exceed the receipt totals, record the overage as a positive amount on the Cash Suspense Receipt under BARS #369.81-Cashiers' Overages and Shortages.
- 3) If the money to be deposited is less than the receipt totals, record the shortage as a negative amount on the Cash Suspense Receipt under BARS #369.81-Cashier's Overages and Shortages.
- 4) Variances must be reported to the Elected Official/Department Head. If the variance exceeds \$50.00, the Elected Official/Department Head must bring it to the attention of the County Auditor. (See Reporting of Losses, pg. 15)
- 5) UNDER NO CIRCUMSTANCES SHALL A COUNTY OFFICE OR DISTRICT MAINTAIN A "SLUSH FUND" OF MONEY TO SUPPLEMENT CASH DIFFERENCES.
- 6) UNDER NO CIRCUMSTANCES SHALL A COUNTY OFFICE OR DISTRICT REMOVE FUNDS TO BE DEPOSITED TO MANIPULATE THE DEPOSIT OR RECEIPT AMOUNTS.

The Treasurer's office will verify the loss and report it to the County Auditor's office (*see reporting of losses, pg. 15).

Recurring Offages

When a loss or overage occurs, regardless of the amount, the Department or District management must make note of it and have a system for reviewing such incidents. Employee theft is the largest unreported loss faced by most businesses and spotting patterns in over/short situations can save thousands of dollars. While a few dollars may seem insignificant, an employee taking small amounts is likely to escalate to large amounts.

Most variances are one-time, accidental, events but having reports and reviewing them significantly increases the chances of seeing patterns in amounts or employees.

A manager seeing, suspecting, or being notified of recurring offages should:

- 1) Create a packet of receipts showing dates, amounts, and employee(s) who generated the over/short receipts.
- 2) Contact the Treasurer's Office to review the data.
- 3) If the pattern appears related to a specific employee, additional actions before a discussion with the employee may include:
 - a. Contacting the HR Department
 - b. Notifying the Auditor's Office
 - c. Seeking guidance from the Prosecutor's Office

If the pattern appears related to a specific customer, transaction type, or dollar amount, planning or procedural changes may be needed to minimize future occurrences. (see Reporting of Losses)

Checking for Counterfeit Bills

When cash is tendered, it is the cash handler's responsibility to review the currency for any potential possible signs of counterfeiting. Best Practice is to check 100% of all bills \$20 and larger.

The methods we use for checking for counterfeit notes are:

- Flashlight: Backlight the security strip.
- Security Strip: Contains the dollar amount of the note and "USA"
 - Example: \$100 bill would have "100 USA 100 USA 100 USA" printed along the security strip
- Fiber Content: US currency paper consists of 25% linen and 75% cotton and contains small randomly disbursed red and blue security fibers embedded throughout the paper.
- Size of the Bill: When bills are jogged, they should be the same size.
- For more information visit: www.uscurrency.gov.

If you are suspicious of a bill presented by a customer, the following procedure is to be observed:

- 1) Notwithstanding the following guidelines, **never do anything that puts yourself at risk;**
- 2) DO NOT return the currency to the passer;
- 3) DELAY the passer, if possible;
- 4) Note the passer's description, the description of any companion, and if possible, the license number of any vehicle used;
- 5) Handle the bill as little as possible in order to preserve any fingerprints, and place it in a protective cover;
- 6) Surrender the bill only to law enforcement authorities;
- 7) Notify the Department Head or Elected Official
- 8) Counterfeit money received by the bank will be recorded as a loss to Kittitas County.

If a cash handler has identified counterfeit documents in their possession without knowledge of their origin, contact Secret Service; they will ask for serial numbers and other identifiers to confirm whether the bill is counterfeit.

Altered Currency

Altering currency is done by taking a genuine bill and tearing off a corner or two of a small bill such as a \$1 or \$5 and then replacing these comers with the corners of a larger bill such as a \$10, \$20 or

\$50 bill. The original larger denomination bill is still redeemed as full value as mutilated money with one or more corners missing. The Treasurer's Office recommends as a standard practice counting currency by looking at the face of the bill, not at the denomination in the corners.

Cash Receipting

Description

BARS GAAP Manual 3.6.1 - All funds, check or cash, must be receipted immediately upon acceptance. All funds and receipts must be placed in a lockable drawer or cash register. The cash register and/or drawer must be kept locked at all times when authorized personnel are not in attendance or within the receipting area.

- All customers must be issued a receipt for all transactions, using only authorized forms (this is for tax payments and department/district deposits)
- Require cashiers to endorse and date-stamp checks immediately upon receipt.
- Each cashier has unique login credentials that should not be shared.
- Each cashier should lock their terminal(s) when they step away.
- Individual cash drawers for each employee who handles cash, with no sharing permitted.
- Balance cash drawer daily with the appropriate documentation.
- Deposits should be made intact to authorized entity accounts only.

Deposits

- 1) Every public officer and employee, whose duty it is to collect and receive payments should deposit receipts with the treasurer of the local government at least once every 24-hours. The treasurer of the local government may grant an exception where such daily transfers would not be administratively practical or feasible (RCW 43.09.240).
- 2) Deposits must be made intact, meaning all payments received must be deposited without substitution. This is evidenced by the composition of checks and cash listed on the deposit slip matched to related receipt records.
- 3) Checks must be restrictively endorsed For Deposit Only immediately upon receipt.
- 4) Separate bank accounts may be used to receipt funds and transfer them to a master account to facilitate the timely collection of cash in remote areas or as part of the government's banking structure. These accounts (which may be referred to as zero-balance, clearing, transmittal or depository accounts), should be swept at least monthly and be independently reconciled the same as all other bank accounts.

Tendering Checks, Check-like items (warrants, money orders, etc.), and Credit/Debit Cards.

The cashier needs to review the check for negotiability. The following are items to look for:

- 1) MICR needs to be pre-printed on the face of the check along with the minimum of the customer's name; preference is the customer's address, city, and state (this information is needed if a refund needs to be generated)
- 2) Current date (if in person).
- 3) Acceptable Payee examples; Kittitas County Treasurer; KCT; Kittitas County Assessor; Kittitas County Auditor; or Kittitas County.
- 4) The amount of the check must appear twice: numerical and written. Financial institutions credit our account from the written legal. **Be sure to enter the check amount tendered from the written legal.** (It is common for customers to omit part of the written legal.)
- 5) **All checks or check-like items must be restrictively endorsed at the time of tendering payment.**

- 6) Once the checks or check-like items are tendered, they need to be secured from the view of customers (placed in a till, drawer, or secured location).
- 7) No two-party or postdated check will be accepted.
- 8) Credit/Debit cards must be present to use as a form of payment (a photocopy is not acceptable). See *Credit Card* chapter.

Receipting

The following information should be included on all receipts:

- Amount of receipt.
- Sequential number of receipt.
- Date of receipt.
- Name of the payee.
- Tender type of funds received (i.e. cash, checks).
- Identification of cashier receiving funds.

- 1) Accepting checks – general guidelines and best practices
 - a. Compare the written amount and the numerical amount. State law says if there is a difference between the two, the written amount is the correct amount for legal purposes. (RCW 62A.3-11 8(b))
 - b. Verify that the check has been signed by the payer.
 - c. Watch for special wording such as "NOT GOOD IF OVER \$1,000" or "VOID AFTER 30 DAYS", as any special instructions written on the check take precedence over Washington State Law.
 - d. Verify that the check is MICR encoded along the bottom edge with the 9-digit Federal Reserve routing number.
 - e. Refuse two-party checks.
 - f. Refuse acceptance of **post-dated checks**.
 - g. Accept checks for the amount owed only. **No change may be given to the customer.**
 - h. Refuse checks written 180 days before the current date as the bank may not redeem any check over this time limit.
 - i. Foreign checks should not be accepted unless the check states "PAYABLE IN U.S. FUNDS."
 - j. **No employee or personal checks, loans or IOU's** may be cashed from any cash drawer, change fund, or petty cash supply.
 - k. A restrictive endorsement should be immediately placed at the top 1.5 inches of the back of any check received. Your office endorsement should be stamped on all checks before deposit with the Treasurer's Office. All departments should use an endorsement stamp like the following:

AUDITOR-LEGALS
PAY TO THE ORDER OF
US BANK OF WASHINGTON
FOR DEPOSIT ONLY
KITITAS COUNTY TREASURER
123456789 12345678901234

- l. When depositing directly into a bank account, other than an account maintained by the Treasurer's Office:

KITTITAS COUNTY SOLID WASTE
PAY TO THE ORDER OF
CASHMERE VALLEY BANK
FOR DEPOSIT ONLY
123456789 12345678901234

Receipting "over-the-counter" payments

- 1) The departments should establish initial control of receipting for "over-the-counter payments" using cash registers or computer software that provides a receipt numbering system, or pre-numbered multi-copy cash receipt forms. **Under no circumstances will unnumbered receipts be used.**
- 2) The department cashiers or accounting clerks will account for all pre-numbered receipt forms that are printed for their department. Voided departmental receipts **will not** be destroyed. Voided receipt forms shall be kept on file in the department.
- 3) All pre-numbered receipt books issued to outside cash handling sites should be logged out, and signed for, by the Elected Official Department Head or his/her designee. The numerical sequence of receipt books should be kept in the proper order to better account for issued receipts.
- 5) Checks must be for the exact amount.
- 6) NO CASH CAN BE GIVEN BACK AS CHANGE TO A CUSTOMER FOR PERSONAL CHECK, COMPANY CHECK, CASHIER'S CHECK, OR ANY CHECK-LIKE INSTRUMENT.

Receipting Payments by Mail

Any payment processing procedure should include a clear record of money received, be processed timely, and identify the cashier handling the processing of mail. The following suggested guidelines should be followed:

- 1) Departments should establish initial control of incoming mail received by implementing the following procedure:
 - a. Two employees should open daily mail and prepare a list of cash and checks received (remittance list), identifying:
 - i. Date check was received.
 - ii. Name of the payee on the check.
 - iii. Check the amount.
 - b. In departments where this procedure is not a viable option, the department should implement a system of supervisory review of the remittance list and bank deposits. (Appendix 2).
 - c. Prepare all payments for immediate deposit with the County Treasurer or bank. Be sure checks are signed.
 - d. Put all unprocessed mail in a secure location, such as a vault or locked cabinet or drawer overnight.
- 2) When receipting payments received in the mail, the following procedures should be observed:
 - a. Using cash registers or computer software that provides a receipt numbering system, or pre-number red multi-copy cash receipt forms. Under no circumstances

- will unnumbered receipts be used.
- b. Departments should process all payments received in the mail **daily**.
- c. Checks received via mail that are over/under the threshold per Kittitas County Resolution #2023-074
 - i. If the funds to be deposited exceed the receipt totals, record the overage as a positive amount on the Cash Suspense Receipt under BARS #369.81- Cashiers' Overages and Shortages.
 - ii. If the money to be deposited is less than the receipt totals, record the shortage as a negative amount on the Cash Suspense Receipt under BARS #369.81- Cashier's Overages and Shortages.
- d. Receiving cash by mail
 - i. The Treasurer's office strongly discourages sending cash through the mail.
 - ii. If cash is received via mail, it must be counted under dual control and receipted immediately.

Internal Controls

Internal control refers to how management runs its organization and achieves organizational objectives. Office of the State Auditor 3.1.3 (Appendix 6).

Internal control is a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations performance
- Compliance with applicable laws and regulations and safeguarding of public resources
- Reliability of financial reporting

The following are the minimum expected controls for cash receipting:

- 1) More than one employee should open the daily mail and prepare a list of cash and checks received (remittance list). If dual custody is not feasible, the department should consider compensating controls such as having mail opened in an area observable by other employees or stronger monitoring controls over revenues.
- 2) Deposits may be prepared by the person who received the payment. The department should implement a system of supervisory review of the remittance list and bank deposits to ensure deposits are made intact.
- 3) Checks received in the mail should be briefly reviewed for accuracy (e.g., proper payee, date, signature of payor, etc.). Checks with obvious inaccuracies should not be included in the deposit. In such a case, the entity should contact the payor and request that the payment be corrected or reissued.
- 4) The daily remittance list should be compared (reconciled) to daily deposit slips and to the cash receipts journal (or check register) regularly. This should be performed by someone other than the employee who prepared the remittance list. Any shortage should be resolved.
- 5) A duplicate copy of the bank-validated deposit slip showing the composition of receipts should be retained by someone other than the employee making up the deposit.
- 6) The bank statement reconciliation should be performed by a person who does not have custody of or access to cash during any point in the receipting and depositing process. This reconciliation should include comparing deposits per bank to recorded receipting transactions in the general ledger.
- 7) Deposits should be physically safeguarded using bank bags with locks or other tamper-proof devices.

- 8) Receipts should be physically safeguarded during the operating day and secured in a safe or vault overnight. Access to the cashiering area should be appropriately restricted whenever possible.
- 9) Access to the safe or vault should be limited, and the combination should be changed periodically. In addition, the safe and vault combination should be changed after employees terminate employment.
- 10) If the department utilizes cash registers, there should be one change fund and one cash register (or drawer) per cashier. This always enables the assignment of responsibility for cash to a specific individual.
- 11) Policies should contain instructions for identifying cash receipts and for dating cash receipts journal entries for that day's receipts.
- 12) Under no circumstances are employees allowed to edit their own receipts. All edited receipts must be completed by a manager and there must be a reason stated in the comment section of the receipt as to why.
 - a. Suspense receipts can only be edited by the Treasurer's office. The treasurer's office must receive the request via email from the manager/supervisor.

Deposits

Departments will submit deposits to the County Treasurer's office within 24-hour of receipt unless a deposit waiver per RCW 43.09.240 has been signed by the department/district and the Treasurer. Deposit requests are submitted electronically through the CAMAS workflow submission process. The Treasurer's Office will provide an electronic receipt through CAMAS, the receipt will be emailed to the person who uploaded the original request.

Off-campus department deposits will be picked up daily by courthouse security. On-campus departments will deliver their prepared deposits to the Treasurer's office. ***See Daily Pickup of County Funds for Bank Deposit, pg. 21.**

Preparing Deposits

Deposits must be verified to the bank account the following business day. Transactions are viewable in the treasury management system as well as online bank statements. For questions about specific transaction postings, contact the Treasurer's Office.

Checks that have been remotely deposited must be retained until the check has cleared and posted to the account. The County recommends the physical check be held longer in case the check is returned or if there is reported fraud per County retention policies and procedures.

1) Prepare a Deposit Slip

Deposit slips are uniquely coded to your department and location, so please use only those deposit slips that Treasury has ordered for your use. Do not share with another department. Deposit amounts are split into three components and then totaled:

- a. Total the Currency (bills)
 - i. Count the currency.
 - ii. Enter the total on the "TOTAL CURRENCY" line. Enter "0" if none.
- b. Total the Coin
 - i. Count the coins.
 - ii. Enter the total on the "TOTAL COIN" line. Enter "0" if none.
 - iii. Place the coin in an envelope.
- c. Total the Checks
 - i. Each check needs to be properly endorsed. This should be done immediately upon receipt of the check. ***Contact Treasury to order endorsement stamps.**
 - ii. Run a tape of the checks.
 - iii. Enter the total on "Line 1" **OR** list each check individually on lines 1 through 26. Use additional lines on the back, if needed.
 - iv. Total Deposit
 - v. Total currency, coin, and check amounts.
 - vi. Enter the total in both TOTAL boxes.
 - vii. This total needs to match your Treasurer's Receipt total.
 - viii. Initial receipt.
 - ix. Keep the yellow copy of the deposit slip for your records.
- d. Date, list department and initial each deposit slip.

2) Bag the Deposit

- a. Name – enter Kittitas County/Your Department/Your Name.
- b. Account #/Location # – leave blank. Information is on the deposit slip.
- c. Said to Contain – enter dollar amounts for Cash, Checks, and Total Deposit.
- d. Date – date of deposit

Currency and coin go into the pocket. Checks go into the pocket with the deposit slip facing the front. Seal both the top and bottom portions of the bag by removing perforated strips.

3) Fill out the deposit log

Complete one line in the log per bag so each bag can be tracked separately:

- a. Date – enter the Courier pickup date.
- b. Time – Security will fill out the time of pick-up
- c. Bag # - number on the deposit bag
- d. Deposit Amount – amount listed on the bag
- e. Employee – name of the employee whose deposit it is
- f. SO Initials – Security Officer initials.

4) Supplies

Contact the Treasurer's office to order endorsement stamps, courier deposit bags, and your uniquely coded deposit slips. Email treasurer@co.kittitas.wa.us or call 509-962-7535.

5) Issues with Deposit or Security

Contact the Treasurer's office to resolve any issues you may experience.

Reporting of Losses

Description

In the event of a suspected loss of public funds, the correct procedures must be followed to minimize the loss. If a loss occurs the following procedures should be followed:

Per RCW 43.09.185 requires that all state agencies and local governments **immediately** notify the State Auditor's Office (SAO) per BARS GAAP Manual 3.10.2 in the event of a known or suspected loss of public funds or assets or other illegal activity.

This guidance should establish an individual responsible for informing managers and employees about these reporting requirements and ensuring the SAO is promptly informed of losses as required. These actions will also help to ensure that:

- Losses are minimized.
- Investigations and audits are not hampered.
- Improper settlements are not made with employees.
- Incorrect personnel actions are not taken.
- Employees are protected from false accusations.
- Bond claims are not jeopardized.

The County should **immediately** notify the appropriate local or state law enforcement agency of the following:

- Suspected losses involving the health or safety of employees or property.
- Losses resulting from breaking and entering or other vandalism of property.

Entities **are not required** to report the following to the SAO:

- Normal and reasonable *over and short* situations from cash receipting operations. Record these transactions in the accounting system as miscellaneous income and expense, respectively, and monitor this activity by the cashier for any unusual trends.
- Reasonable inventory shortages were identified during a physical count. Record inventory adjustments in the accounting system.
- Breaking and entering or other vandalism of property.

Offices/Departments should notify the Treasurer's Office when there is a net loss of \$50 or more on any single transaction, cash drawer, or over the course of a calendar month for one employee. (Appendix 3)

The Treasurer's Office will verify the loss. If a net loss is verified, the Treasurer's Office will notify the Department Head, Elected Official or their designee and the County Departments will take the following action(s):

- 1) Notify appropriate entity managers who are not involved in the loss. This may include the Elected Official/Department Head, their designee(s), the appropriate supervisors and internal finance/admin staff, depending upon the circumstances. Providing notification to your legal counsel may also be appropriate.
- 2) Do not enter into a restitution agreement with an employee prior to an audit to establish the amount of loss in the case.

- 3) Ensure that any personnel action is taken based on the employee not following entity policies and procedures, rather than for misappropriating public funds (civil versus criminal). File a police report with the appropriate local or state law enforcement agency when advised to do so by the County Auditor.

Once notified by the Treasurer regarding a net loss, the Auditor's Office will take the following actions:

- 1) Report the loss to SAO online or to the Audit Manager
- 2) Consolidate and protect the accounting records from loss or destruction. All original records related to the loss will be secured in a safe place, until SAO has completed an audit and the appropriate retention requirements are met. The Auditor will also retain the completed loss reporting form.
- 3) Consult with Human Resources and the County Prosecuting Attorney to advise the County Department Head/Elected Official on next steps in resolving the issue, including any recommended civil or criminal actions related to the loss.

Do not attempt to correct the loss without reporting to the authorities identified above. In addition, RCW 43.09.260 requires written approval of the State Auditor and Attorney General before state agencies and local governments make any restitution agreement, compromise, or settlement of loss claims covered by RCW 43.09.185.

Petty Cash

Description

Per Guidance SAO BARS GAAP Manual 3.8.8 in this section applies to petty cash, imprest accounts, working funds, advance travel, stamp funds, change funds, or any other revolving funds set aside for facilitating minor disbursements, making change, and similar uses. When revolving funds are disbursed, they are restored to the authorized balance by a warrant drawn and charged to the applicable fund.

Petty cash includes change funds, till accounts, revolving funds, advanced travel, and any money or other funds set aside for such specific purposes as minor disbursements, making change, or similar use. If petty cash is disbursed, it may be restored to its beginning balance twice monthly by a warrant drawn and charged to the appropriate operating fund. The amount of the warrant should always be equal to the amount of the disbursements.

- 1) The Board of County Commissioners must authorize the establishment of each petty cash account by resolution, submitted to the Board by the County Auditor's Office. Likewise, subsequent increases or decreases in the imprest amount.
- 2) A custodian of the account shall be appointed by the Board of County Commissioners, or a County Board/Commission as designated in resolution. The custodian shall not relate to the processing of invoices, check signing, general account, or cash receipt functions within the specific department, organization, or event.
- 3) The custodian shall ensure the petty cash is always kept in a safe and secure location.
- 4) It is the responsibility of each department to ensure that their petty cash account is periodically reconciled by personnel other than the custodian of the account. The County Auditor, or his/her designee, may perform audits of each department's petty cash accounts as deemed necessary.
- 5) The imprest amount shall be established by issuing a warrant. When established by warrant, the transaction is a non-budget item.
- 6) The authorized amount of all petty cash must be accounted for on the County's Balance Sheet.
- 7) If petty cash is disbursed, it must be replenished a minimum of one time per month. This action is subject to the same review and approval process as invoices. The replenishment of the petty cash account must be vouchered with the appropriate original receipts attached. These receipts must include:
 - a. Date
 - b. Amount
 - c. Recipient
 - d. Purpose of each disbursement
- 8) Receipts must be signed by the person receiving funds. Receipts should be perforated or canceled by some other means to prevent reuse. At the time of replenishment, the custodian must ensure the balance remaining in the petty cash fund, together with the replenishment voucher, equals the authorized imprest account.
- 9) The petty cash account may NOT be used to reimburse an employee from these funds, regardless of the situation.
- 10) The petty cash account may NOT be used for personal cash advances, regardless of the situation.

- 11) Petty cash accounts should always be replenished to their original levels at the end of each fiscal year. This will ensure all expenses are reflected in the proper accounting period.
- 12) When an individual's appointment as custodian has ended, the fund must be replenished to its original balance and the imprest amount turned over to the disbursing officer. The County Auditor must then be notified of the change in custodian, and his/her designee will be responsible for performing an audit.

Bank Returned (NSF) Checks

Description

Each department head and elected official is authorized to charge a fee of \$35.00 for all checks returned by the bank. As the bank charges a fee to the Treasurer's Checking Account for each deposited item returned, the Treasurer's Office is authorized to assess an NSF Processing Fee of \$10.00 directly to the Department, Board, Committee or Elected Official that originally receipted the check.

Checks may be returned due to insufficient funds, closed accounts, invalid signatures, stop payments, or any other conditions making the checks invalid.

- 1) If a check is returned by the bank, the Treasurer's Office will contact the department that originally receipted the funds and request a Cash Suspense Receipt from them denoting the BARS number that is to be debited. Once this information is received, the Treasurer's Office will process a "red receipt" (debit) to the department's funds. The Treasurer's Office will also assess the department's fund an NSF Processing Fee of \$5.00. Departments that have legislative or court-directed procedures for NSF checks are exempt from the following procedures (such as a District and Superior Court).
- 2) Departments may elect to require payment of the returned check and applicable fees in the form of cash, money order, or cashier's check.
- 3) Collection action taken by the department should include any suitable action necessary, such as the revocation of the license or permit, and/or suspension of all further service with the remitter until payment of the original check amount, plus all applicable fees have been received. Each department should adequately document any action taken.
- 4) A letter should be sent to the remitter to notify them of the returned check. The letter should include notice of the applicable NSF fees, required mode of payment, and detailed information on any action taken to revoke the license or permit, and/or to stop service.
- 5) Departments may elect to maintain a list of parties who have had checks returned by the bank and establish an internal policy for refusing personal checks from any party on the list.

Non-County Money

Monetary Gifts

Any monetary gifts to the County received by a county official, employee, or agent from a known benefactor.

- An official county receipt for all monetary gifts should be given for face-to-face transactions.
- Deposit all gifts in the County Treasurer's Office in exchange for a receipt.
- Provide the County Treasurer with a memo outlining the factors associated with the receipt of the gift and any associated documentation.

Donation

A sum of money given to the county anonymously or an error that cannot be returned.

- County officials, employees, or agents who obtain a donation of money to the county are responsible for receiving, safekeeping, and depositing those donations.
- A receipt will be written when the donation is deposited with the County Treasurer.

Found Property

Non-County money found by a county official, employee, or agent, while performing county duties.

- Any county officer, employee, or agent who finds non-county money while performing county duties, shall immediately turn in the money and a report to the security desk at the courthouse.

Non-County Funds

Non-County funds (e.g., Fire House funds, coffee funds, "Friends Of" accounts for County parks) are not to be deposited in County accounts.

- All non-County funds are to be kept separate from any County funds.
- The County assumes no responsibility for non-County funds or their loss.
- Only the County Treasurer is authorized to open County bank accounts in the County's name and/or linked to the County's Tax ID.
 - At the request of the County Treasurer, any non-County fund that is inappropriately or incorrectly linked to the County's Tax ID number will be closed within 72-hours.

Daily Pickup of County Funds for Bank Deposit

Description

Per RCW 36.29.010 the Treasurer may provide certain collection services for county departments as it is the duty of all entities where money received for whom the county Treasurer serves as treasurer must be deposited within twenty-four hours in an account designated by the county treasurer unless a waiver is granted by the county treasurer per RCW [43.09.240](#).

Deposits

For the safety and security of Kittitas County staff, a member of the Kittitas County Courthouse Security Team will pick up securely sealed, tamper-proof deposits from off-site county departments/offices daily. Deposits are to be ready for pick-up by 10:00 a.m. These offices will include, but may not be limited to: Solid Waste, Public Health, CDS, Public Works, Event Center, Sheriff's office, and Jail. Bail will be deposited directly to the bank.

Departments/offices located at the main county courthouse will deliver their deposit(s) in securely sealed, tamper-proof deposit bags to the Treasurer's office daily by 9:30 a.m. These offices include the Auditor, Clerk, and Lower District Court.

Departments/offices having infrequent deposits are an exception, those offices may continue to bring their deposit to the Treasurer's office for deposit. These offices include Human Resources, Assessors, Prosecutor, and Board of County Commissioners.

All deposit details must be uploaded to the Treasurer's workflow page online, failure to submit your electronic receipt will result in funds being placed in suspense. It will be the responsibility of each department to track their funds.

Deposits will be placed in a securely sealed, tamper-proof bank bag along with a deposit slip placed in the bag. All staff responsible for preparing a daily deposit will be trained by the Treasurer's office. Off-site departments will also prepare a receipt log, provided by the Treasurer's Office, to be filled out for accuracy and ease of reading, including Date, Bag Number(s), Deposit Amount(s), Pickup Time (to be filled in by a Security Deputy), and Security Deputy's Signature. These forms are to be included with, but outside of, the sealed bags to be delivered to the bank. It will be the department's responsibility to retain the spreadsheet of deposit activity for a minimum of one year.

Deposits must be kept in a locking safe/drawer until they can be picked up. Keys and/or the combination to the locking drawer or safe should be limited to select employees. Keys should be kept out of public access. These keys should never leave the office (i.e. go home with an employee). The combination must be changed when an employee with knowledge of the combination terminates employment. Each department/office will provide the Treasurer's office and County Security with the name(s) of authorized personnel in each department responsible for the deposit and where the deposit will be located. Employees should always verify the identity of the security personnel each time the funds are released. Do not release any deposit to security if there are any questions or problems; simply state "the deposit is not ready" and contact the Security desk at 777 and/or the Treasurer's office at (509) 962-7535.

The Security Deputy shall review the log for accuracy before signing. By signing the log, the Security Deputy accepts responsibility for delivery of the same to the Ellensburg Branch of U.S. Bank on the same day of acceptance. The Security Officer shall not be considered responsible for any inaccuracies within the delivered tamperproof bags if the bags are delivered to the bank intact.

The Security Deputy is not required to remain in attendance at the bank while the bag contents are processed, all deposits other than the Auditor's DOL deposit will be placed in the bank's drop box. The bank will process the deposit, and if discrepancies are found by the bank or while processing at the Treasurer's office, we will notify your department to rectify the deposit.

Safeguarding Funds in an Emergency

Description

In the event an emergency occurs and/or the evacuation of the department or work site is required, all funds must be secured in a locked location. This should take place only after determining the safety of all employees within the department. These precautions shall be the responsibility of the Elected Official/Department Head.

Robbery

A robbery is a person-on-person crime that occurs when an offender takes something of value by force or threat of force. Because it is a serious risk to employees, it is important to train employees and implement strategies to mitigate risk. The average robbery takes ninety seconds from start to finish, so be prepared to react quickly.

Procedures to follow **during*** a robbery:

- 1) Always assume that there is a weapon, even if you don't see one.
- 2) Be polite and accommodating. Do not upset or antagonize the suspect. The calmer you are, the calmer the suspect will remain.
- 3) Keep talking to the suspect. Explain your every movement. Avoid making any quick movements that might alarm the suspect.
- 4) Do exactly as the suspect asks.
- 5) Observe any distinguishing features/mannerisms of the suspect. Try to remember the distinguishing features of the robber, as part of the subsequent investigation will involve law enforcement asking you to describe the robber.
- 6) Note any evidence left by the suspect – anything touched, dropped, or left behind.
- 7) Listen to the voice, inflections, slang, or names that the robber uses.
- 8) Do not leave the premises or call "8" 911 until it is safe to do so.

* Offices/Departments located within the Courthouse should, if possible, without endangering yourself or others alert Courthouse Security. Your office/department should refer to your emergency preparedness guide for your specific procedures.

Procedures to follow **after*** the robbery:

- 1) Call 911 and stay on the line until law enforcement officers arrive.
 - Offices/Departments off-site should call 911 as soon as possible. Courthouse Security should be notified after 911 has been called.
- 2) Close your cash register or drawer, lock the entrance door, and notify your immediate supervisor of the robbery.
- 3) No one except law enforcement officers and your department officials should be allowed on the premises after the robbery.
- 4) Secure the entire robbery scene as best you can until law enforcement arrives.
- 5) Do not attempt to impede the suspect in any way. Any such action may put you or others' lives/safety in jeopardy.
- 6) Be observant but not obvious.

Fire or natural disaster

In any emergency, remember your safety and any human safety is more important than County Funds.

In the case of fire or natural disaster, please refer to the County's building-specific Emergency Action Plan as well as any written departmental emergency procedures. The emergency procedures to be followed at the cash handler's specific facility should be discussed and approved with the department management, and the cash handler should know where all the exits are in the facility.

CHAPTER 2:

Credit Card Policy and Procedures

Purpose

Acceptance of payment by credit/debit cards has proven to have benefits such as, but not limited to ease of use through electronic technology, mail, and processing float reduction, improvement in funds availability, less risk associated with defective checks, reduced delinquent collections, more timely payments, and reduced interest and penalties for customers.

The purpose of this policy is to establish business policies and procedures for accepting credit and debit cards in Kittitas County. The policy will minimize risk and provide the greatest value, security of data, and availability of services to our customers within the rules and regulations established by the Payment Card Industry (PCI) and articulated in the PCI Data Security Standards (DSS). Additionally, these processes are intended to ensure that payment card acceptance procedures are appropriately integrated with Kittitas County's accounting and other systems.

This policy applies to all Kittitas County employees, departments, offices, or officials who, while doing business on behalf of Kittitas County, accept credit or debit cards or otherwise process, transmit, or handle cardholder information in physical or electronic format.

Summary Statement

County departments may accept credit or debit cards for payment of services or goods unless prevented by statute or other policies. When any County department or office plans to accept credit or debit cards as a payment method, the Treasurer must be informed, and the Treasurer's office will assist in that process. Districts for whom the Treasurer acts as the ex officio treasurer should also consult with the Treasurer before negotiating a contract to accept and process credit or debit cards. Final plans must be approved by the Treasurer before implementation and Department Head/Elected Officials must work with the Information Technology Department to ensure PCI compliance.

Any fees charged to the county including but not limited to equipment, monthly merchant fees, etc. will be debited by the Treasurer from the appropriate fund.

Acceptable Credit or Debit Cards

Kittitas County currently accepts VISA, MasterCard, Discover, and American Express cards and has negotiated contracts for processing Credit or Debit card transactions. Individual Kittitas County employees may not use or negotiate individual contracts with these or other Credit or Debit card companies or processors. All Kittitas County entities must work with the Treasurer's Office to negotiate a contract for credit card processing.

Prohibited Credit or Debit Card Activities

Kittitas County prohibits certain credit card activities that include, but are not limited to:

- Accepting Credit or Debit cards for cash advances
- Refunds more than the original sale amount

- Discounting training or service based on the method of payment.
- Adding a surcharge or additional fees other than those posted to Credit or Debit card transactions

Credit or Debit Card Fees

Each credit or debit card transaction will have an associated fee charged by the credit card company. Fee(s) must be posted at the point-of-sale terminal location.

Per RCW 36.29.190 a payer using electronic payment must pay the transaction processing fee except in certain circumstances outlined in the RCW.

If a department chooses not to charge the transaction processing fee the county department or taxing district must seek approval from the county legislative authority, or the legislative authority of the district where the county treasurer serves as ex officio treasurer.

Refunds

If it is found that a credit card charge was processed in error a refund may be processed. The refund must be credited back to the account that was originally charged. Refunds over the original sale amount or cash refunds are prohibited.

Chargebacks

Occasionally a customer will dispute a credit or debit card transaction, ultimately leading to a chargeback. In the case of a chargeback, the Kittitas County Treasurer's Office will be responsible for distributing chargebacks to the appropriate departments for proper correction.

Maintaining Security

In response to increasing incidents of identity theft, the major payment card companies created the Payment Card Industry Data Security Standard (PCI DSS) to help prevent the theft of customer data. PCI DSS applies to all businesses that accept payment cards to procure goods or services. Compliance with this Standard is enforced by the payment card companies. Generally, noncompliance is discovered when an organization experiences a security breach that includes cardholder data.

Security breaches can result in serious consequences for Kittitas County, including the release of confidential information, damage to reputation, the assessment of substantial fines, possible legal liability, and the potential loss of the ability to accept payment card and eCommerce payments. Kittitas County will make every effort to ensure that Data Security Standards are adhered to. The Kittitas County PCI Compliance Monitoring Process is outlined in Appendix 4.

- Departments and administrative areas accepting credit or debit cards on behalf of Kittitas County are subject to the Credit or Debit Card Industry Data Security Standards (PCI DSS).
- Email should not be used to transmit credit card or personal payment information.
- Kittitas County requires that all external service providers that handle credit or debit card information be PCI compliant.

- Kittitas County restricts access to cardholder data to those with a business "need-to-know."
- For electronic media, cardholder data shall not be stored on servers, local hard drives, or external (removable) media including floppy discs, CDs, or thumb (flash) drives unless encrypted and otherwise in full compliance with PCI DSS. For paper media, cardholder data shall not be stored.
- Credit card or personal information is never downloaded onto any portable devices or media such as USB flash drives, compact disks, laptop computers, or personal digital assistants.
- The processing and storage of personally identifiable credit cards or payment information on Kittitas County computers and servers is prohibited.
- Only secure communication protocols and/or encrypted connections to the authorized vendor are used during the processing of eCommerce transactions.
- Ensure that POS systems are secure, up-to-date, and compliant with industry standards.
- The three or digit four-digit validation code, or full contents of any track data from the magnetic stripe, personal identification number (PIN), or encrypted PIN block are never stored in any form.
- All media containing credit, debit card, or personal payment data must be destroyed when retention time is met.
- The Treasurer must be notified immediately in the event of suspected or confirmed loss of cardholder data. Details of any suspected or confirmed breach should not be disclosed in any email correspondence.

Wireless Technology

Kittitas County will use wireless technology to process or transmit cardholder data over a secured network. Kittitas County employees will never transmit cardholder data over an unsecured network. The storage of cardholder data on local hard drives, floppy disks, or other external media is prohibited. It is also prohibited to use cut-and-paste and print functions during remote access.

Sanctions

The Treasurer may suspend the credit card account privileges of any Kittitas County department not in compliance with this policy or that places Kittitas County at risk.

Training

Department Heads/Elected Officials will be responsible for the training of office personnel in the use of equipment and all proper steps associated with credit or debit card transactions including daily balancing and the importance of accuracy. All employees who will be given access to cardholder data must undergo comprehensive training on credit card processing procedures, including security protocols and customer interaction. After training each employee will be required to sign the Credit Card Policy Acknowledgement Form (Appendix 8) before being allowed to process credit card transactions. It is recommended that one employee act as a lead trainer for all employees utilizing this service.

Processing Procedures

Credit or debit cards may be accepted when the cardholder is present in person or through an online payment portal. Acceptance and processing of credit or debit cards over the telephone is prohibited.

A daily accounting process must be established to reconcile and record credit or debit card transactions. The daily reporting of this must be provided to the Treasurer by 9:30 am each day.

An approved Technologies and Devices form must be filled out by each department or office. This form can be found in Appendix 8.

Only authorized cashiers, designated by department management, are permitted to process credit card payments.

Credit card transactions should be handled in a secure environment with as much privacy as possible.

Separate office balancing duties from credit card processing to prevent errors or fraudulent activities.

Guidelines

- The identity of the customer must be verified before processing any credit card transaction.
- Check the signature on the credit card against a government-issued identification card.
- Process credit card transactions only after receiving proper authorization.
- When the transaction has been approved, two copies of the receipt must be printed; the signed original will be kept by the department or district, and the second copy given to the customer.
- If a transaction is declined, follow established procedures for informing the customer discreetly.
- If a refund is necessary, obtain proper authorization from management and document the reason for the refund.
- Be vigilant for signs of potential fraud, such as multiple declined transactions or suspicious behavior.
- Report any suspicious activity immediately to the supervisor and the County Treasurer.
- Daily balancing of all transactions must be completed at the end of the day or the next morning before beginning to accept new transactions.
- Daily reporting of all credit or debit card activity must be provided to the Treasurer's Office before 9:30 am the next business day.

Department Responsibilities

- Funding the initial equipment lease.
- Installation of equipment and training of employees.
- Ensuring that all employees, contractors, and agents with access to credit or debit card data acknowledge on an annual basis and in writing that they have read and understood this policy. These acknowledgments should be submitted, as requested, to the Treasurer's Office ensuring that all credit or debit card data collected by the department while performing Kittitas County business, regardless of whether the data is stored physically or electronically is secured.

- Management of the system, including but not limited to; required receipting, procedures, refunds, chargebacks, reconciliation, reporting, and communication with the processor.
- Resolving and/or collecting disputed or returned items.
- Immediately notify the Treasurer in the event of suspected or confirmed loss of cardholder data. Details of any suspected or confirmed breach should not be disclosed in any email correspondence.

Treasurer Responsibilities

- Work with external vendors to coordinate credit or debit card policies, standards, and procedures.
- Review and modify the Application for Credit or Debit Card Account Acquisition or Change as necessary.
- Conduct Internal Auditing to:
 - Periodically review Kittitas County employee compliance with this policy and the Credit or Debit Card Industry (PCI) Data Security Standards (DSS).
 - Identify unapproved payment applications or external vendors that collect credit or debit card data on behalf of the county.

Information Technology Responsibilities

- When required, conduct Kittitas County's PCI DSS Self-Assessment and complete the Kittitas County Attestation of Compliance.
- Assist with Department PCI Compliance needs.

CHAPTER 3:

EFT Policy and Procedures

Background

As authorized by RCW 39.58.750, the Kittitas County Treasurer's Office can receive, disburse, or transfer funds through wire or other electronic communication. The Kittitas County Treasurer's Office has established the following policies and procedures per the State Auditor's BARS GAAP manual, 3.6 EFT – Receipts, and 3.8 EFT – Disbursement.

Statement

The use of EFT or ACH will ordinarily only be used as a method of payment to government agencies, vendors and for county payroll. All other use of EFT or ACH transfers will be on a very limited and approved basis by use of forms that provide safeguards. Approval will be provided by the Kittitas County Treasurer's Office along with the department involved.

Non-Kittitas County agencies will not be allowed to process EFT or ACH payments using bank accounts that fall under the Kittitas County umbrella. They will be required to establish a bank account, separate from the Kittitas County umbrella, using their own EIN.

Processes and Instructions

ACH Processing

Kittitas County Treasurer's Office staff with ACH bank permissions are the only persons authorized to set and approve ACH transactions within the Treasurer's Concentration account, except for Auditor payroll transactions, as described below.

Staff in the Kittitas County Auditor's Office accounting department are allowed to initiate ACH payments for payroll and payroll-related vendors directly on the banking platform. Payroll and payroll-related payments may only be approved by a Treasurer's Office staff member with the appropriate permissions. Permission to access, set, and approve ACH Transactions within the banking platform must be approved by the Kittitas County Treasurer. A token will be assigned to each person with ACH permissions.

All ACH payments must be dually authorized by two parties. ACH approvals will only be done by a staff member of the Treasurer's Office after a thorough review of required documentation.

Departments are responsible for uploading transaction requests directly to the Treasurer's workflow page using the CAMAS Cashtax Submission form.

Districts are responsible for uploading transaction requests directly to the Treasurer's workflow page using the forms tab on the Treasurer's public website.

ACH transactions are only processed if requested by the department or district through one of the above two means. It is the requestor's responsibility to verify all payment information in the request

is accurate. ACH requests shall be submitted two business days in advance of the actual transaction date. The daily cutoff time for ACH setting and approving within the Treasurer's Office is 3:30 PM. ACH submissions submitted after 3:30 PM will be processed the next business day. Same-day ACH transactions will be completed on a case-by-case basis and at the discretion of the Treasurer's Office. The Treasurer's Office has set a same-day ACH cutoff of 10:00 AM.

Prior-day ACH activity is reconciled each business day during the regular bank reconciliation process. Unidentified transactions are communicated to the Treasurer's Office management and researched. All suspicious transactions are immediately communicated to US Bank Commercial Customer Service.

Domestic External Wires

Like ACH payments, wire transfers must be dually authorized by two staff members of the Treasurer's office. Only Kittitas County Treasurer's Office staff members with wire permissions may set and approve wire transfers. The Treasurer, Administrative Supervisor, and Finance Officer in the Treasurer's Office are the only persons who are authorized to initiate wire transfers. Other staff may be able to approve. A wire pin is provided to those who are authorized to initiate wire transfers.

Generally, wire transfers are only used under special circumstances. Wire transfer requests must be received no later than five business days before the transaction date to allow the Treasurer's office staff adequate time to verify information and cash flows before the release of funds. A request by the department head, elected official, or district business manager (or equivalent) on department or district letterhead with wiring instructions is required. The letter should also include the reason for the wire and who verified the authenticity of the request. Requests will be verified with the district's business manager (or equivalent) via phone. It is important to keep your contact information up-to-date with the County. The request must be reviewed and approved by either the Treasurer or the Finance Officer prior to the release of funds.

International External Wires

International wires are generally not an approved way to transmit money to vendors as sending money internationally carries more risk—once money leaves the United States, it is unlikely it can be retrieved.

International wires, if required, will be done on a case-by-case basis with prior approval from the Treasurer. International wire transfer requests must be received no later than 14 business days before the transaction date to allow the Treasurer's Office staff adequate time to verify information and cash flows before the release of funds. A request by the department head, elected official, or district business manager (or equivalent) on department or district letterhead with wiring instructions is required. The letter should also include the reason for the wire and who verified the authenticity of the request. Requests will be verified with the district's business manager (or equivalent) via phone. It is important to keep your contact information up-to-date with the County. The request must be reviewed and approved by either the Treasurer or the Finance Officer before the release of funds.

Book Transfers

Book Transfers are internal account transfers and are processed daily through the Treasurer's online banking portal. Departments and districts that have bank accounts listed under the Treasurer's banking umbrella may make deposits into their account and request to deposit money with the Treasurer daily or weekly, depending on their deposit waiver status.

Treasurer's Banking Information Requests

The Treasurer understands that many vendors are not issuing checks any longer and are instead requiring bank information for EFT deposits. You may request banking information from the Treasurer's office for vendor deposits, however, the banking information provided may only be used for the designated vendor. The Treasurer's office tracks each request by entity. Banking information will not be given for reimbursement of travel expenses for individuals employed by the county.

When vendor deposits are being made directly to the Treasurer's account, a notice of deposit via cash suspense receipt (*department*) or cash transmittal (*district*) must be sent to the Treasurer's office by 12:00 PM, two days before receipt of the funds. If funds are deposited into the Treasurer's account and the proper notice is not received from the department or district within (24) hours of funds being received, the funds will be returned to the remitter.

Fraud Protection and Safeguard Procedures

All accounts are required to have ACH debit filters to block all unauthorized ACH draft attempts. Vendors may be added to the county's ACH debit filter with approval from the Treasurer or the Finance Officer.

The Treasurer's office must notify the bank immediately after seeing any suspicious activity received or drawn from the Treasurer's accounts.

Money sent in error will not be returned by any department or district via ACH, wire, or check, rather we will work with US Bank to initiate a return of the transaction as a whole.

ACH and/or wire information updates provided by a vendor or employee must be verified before any money is sent using the new information. Information should be verified using the vendor or employee's contact information currently on file with the county before the updated information is entered.

Appendices

Appendix 1: Recognizing Currency and Coin

The Federal Reserve Bank of the United States has the responsibility for issuing currency for the United States. US currency takes the form of notes engraved on special paper and comes in seven denominations, each being a portrait of a different famous American.

DENOMINATION	PORTRAIT
\$1	George Washington
\$2	Thomas Jefferson
\$5	Abraham Lincoln
\$10	Alexander Hamilton
\$20	Andrew Jackson
\$50	Ulysses S. Grant
\$100	Benjamin Franklin

In addition, the face of the bill contains key elements such as the denomination, Federal Reserve Bank Seal, serial number, and Treasury Department seal. The reserve side of a bill is similar for all denominations. The value designation differs, but also appears in ten places. In the center of the bill, under the words, "In God We Trust", appears the Great Seal of the United States.

In looking at a dollar bill, you will notice the following:

- The value of each bill is numerically posted in all four corners on both sides.
- The value is written out across the bottom of the face side.
- The Federal Reserve Seal appears to the left of the portrait. The Treasury Seal appears to the right of the portrait, embossed over the written dollar amount.
- The unique serial number of the bill appears both in the lower left portion and upper right portion on the face of the bill.
- The number of the Federal Reserve District that issued the bill appears near all four corners on the face of the bill.

Currency is usually strapped in the following amounts:

DENOMINATION	BAND	STRAP
100		\$1,000
50		\$1,000
20	\$500	\$2,000
10	\$250	\$1,000
5	\$100	\$500
2	\$50	\$200
1	\$25	\$100

The coin is wrapped in the following amounts:

DENOMINATION	AMOUNT
\$1.00 (Eisenhower)	\$20.00
\$1.00 (Susan B. Anthony)	\$25.00
\$0.50	\$10.00
\$0.25	\$10.00
\$0.10	\$5.00
\$0.05	\$2.00
\$0.01	\$0.50

Appendix 2: How to Control Cash in a Small Office






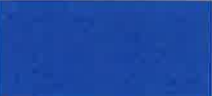



Often it is difficult to divide duties in a small office so there are adequate controls over cash. The information below is designed to aid in completing the required work in small offices.

Legend: ★ Person to perform the duty ■ Person should NOT perform the duty
Backups can perform task with ★

Two Person Office	Person 1	Person 2
Receive cash/check from customers, prepare cash receipt report	★	■
Prepare and make deposits to the Treasurer's office and/or bank	★	■
Post activity to the check register and/or financial records from the cash receipt book and original purchasing documents, making sure purchases have been properly approved.	■	★
Keep possession of the checkbook and/or have access to blank checks	★	■
Prepare check requests	★	Backup – cannot approve check requests prepared by self
Approve check requests, making sure to review supporting documentation (invoice, receipt, etc.)	Backup – cannot approve check requests prepared by self	★
Sign checks, making sure the request is complete and approved.	★	■
Balance/reconcile check register/books to the bank statement each month	■	★
Review the bank reconciliation, making sure that the ending balance on the check register agrees to the adjusted balance on the checking account statement	Backup	Send to a central office to be reviewed, or have Person 1 review the work

Note: It is important to follow all the boxes correctly to have an adequate segregation of duties. Lack of segregation of duties increases the risk of loss to the County. If your department cannot accommodate these guidelines, your office/department cash handling policy must address Treasurer approved alternatives.

Legend: ★ Person to perform the duty  Person should NOT perform the duty
 Backups can perform task with ★

Two Person Office	Person 1	Person 2	Person 3
Receive cash/check from customers, prepare cash receipt report	★		Backup
Prepare and make deposits to the Treasurer's office and/or bank	★		Backup
Post activity to the check register and/or financial records from the cash receipt book and original purchasing documents, making sure purchases have been properly approved.		★	Backup
Keep possession of the checkbook and/or have access to blank checks	Backup		★
Prepare check requests	★	Backup – cannot approve check requests prepared by self	
Approve check requests, making sure to review supporting documentation (invoice, receipt, etc.)	Backup – cannot approve check requests prepared by self	cannot approve check requests prepared by self	★
Sign checks, making sure the request is complete and approved.	Backup		★
Balance/reconcile check register/books to the bank statement each month		★	
Review the bank reconciliation, making sure that the ending balance on the check register agrees to the adjusted balance on the checking account statement	Backup		★
Have access to blank checks	Backup		★

Note: It is important to follow all the boxes correctly to have an adequate segregation of duties. Lack of segregation of duties increases the risk of loss to the County. If your department cannot accommodate these guidelines, your office/department cash handling policy must address Treasurer approved alternatives.

Appendix 3: Reporting a Loss

Any revenue loss or overage over \$50.00 must be reported to the Department Head/Elected Official, then to the Kittitas County Auditor (according to the Kittitas County Cash Handling Policy). The submission should include all relevant information and documentation.

Date of occurrence: _____ Department: _____

Overage Amount: _____ Shortage Amount: _____

Employee(s) involved: _____

Explanation of overage/shortage: _____

Was activity leading to overage/shortage per the Kittitas County Cash Handling Policy?

Yes: _____ No: _____ (if no, please explain): _____

How could the overage/shortage have been avoided? _____

What steps will be taken to prevent such an occurrence from re-occurring? _____

Reported by: _____

Department Head/Elected Official:

_____ Date

Received by: _____

Kittitas County Auditor

_____ Date

Appendix 4: PCI Compliance Monitoring Process for Kittitas County

Objective: This process establishes a systematic approach for monitoring PCI compliance across all departments within Kittitas County to ensure the secure handling of credit and debit card information.

- 1) **Designation of Compliance Officer:**
 - a. The County Treasurer shall designate a PCI Compliance Officer responsible for overseeing PCI compliance across all departments.
 - b. The Compliance Officer will collaborate with the Information Technology Department to fulfill their responsibilities.
- 2) **Establishing a PCI Compliance Team:**
 - a. The Compliance Officer will assemble a PCI Compliance Team comprising representatives from the Information Technology Department and relevant department heads.
 - b. The team will work collectively to implement and monitor PCI compliance.
- 3) **Inventory of Systems and Processes:**
 - a. The Compliance Officer, in collaboration with the Information Technology Department, will maintain an inventory of systems and processes involved in credit and debit card transactions across all departments.
 - b. The inventory will include hardware, software, point-of-sale (POS) devices, and any other components that handle cardholder data.
- 4) **Conducting Risk Assessments:**
 - a. Regular risk assessments will be conducted to identify potential vulnerabilities and threats associated with systems and processes handling cardholder data.
 - b. Identified risks will be prioritized, and mitigation strategies will be developed.
- 5) **Compliance Training and Awareness:**
 - a. The Compliance Officer will ensure that employees handling credit and debit card information undergo regular PCI compliance training.
 - b. Awareness programs will be conducted to keep staff informed about the importance of PCI compliance and the potential risks associated with non-compliance.
- 6) **Implementing Security Controls:**
 - a. The Information Technology Department will collaborate with departments to implement necessary security controls outlined in the PCI DSS standards.
 - b. Security controls may include encryption, access controls, network security, and regular security audits.
- 7) **Annual Compliance Audits:**
 - a. The Compliance Officer, in coordination with the PCI Compliance Team, will conduct annual compliance audits to assess adherence to PCI DSS standards.
 - b. Audits will include both technical assessments and procedural reviews.
- 8) **Vendor Management:**
 - a. The Compliance Officer will establish a vendor management process to ensure that third-party vendors involved in electronic payment processing comply with PCI DSS standards.
 - b. Contracts with vendors will include provisions for regular security assessments.
- 9) **Incident Response Plan:**
 - a. A comprehensive incident response plan will be developed and maintained to address any security incidents related to credit and debit card information.

- b. The plan will include procedures for reporting and investigating security incidents promptly.
- 10) **Documentation and Record-Keeping:**
 - a. The Compliance Officer will ensure that all departments maintain detailed records of PCI compliance activities, including audit reports, training records, and incident response documentation.
 - b. Records will be retained per applicable record-keeping regulations.
- 11) **Periodic Reporting to Management:**
 - a. The Compliance Officer will provide periodic reports to the Treasurer, summarizing the status of PCI compliance.
 - b. Reports will include an overview of activities, identified risks, mitigation efforts, and recommendations for improvement.
- 12) **Continuous Improvement:**
 - a. The PCI Compliance Team will engage in continuous improvement efforts based on audit findings, emerging threats, and changes in PCI DSS standards.
 - b. Feedback from compliance audits will be used to refine and enhance security controls and procedures.
- 13) **External Audits and Assessments:**
 - a. External audits and assessments may be conducted periodically by qualified third-party assessors to validate internal compliance efforts.
 - b. The Compliance Officer will coordinate and facilitate external assessments.
- 14) **Policy Review and Updates:**
 - a. The Compliance Officer, in collaboration with the PCI Compliance Team, will review and update PCI compliance policies and procedures regularly.
 - b. Updates will be made in response to changes in PCI DSS standards or because of internal assessments.
- 15) **Communication of Non-Compliance:**
 - a. In the event of non-compliance, the Compliance Officer will promptly communicate findings to relevant department heads, senior management, and the Board of County Commissioners.
 - b. Corrective action plans will be developed and implemented to address identified issues.

This PCI Compliance Monitoring Process ensures a proactive and comprehensive approach to monitoring PCI compliance across multiple departments within the Kittitas County Government. The process aims to safeguard cardholder data, mitigate risks, and continuously improve security measures. All departments are expected to actively participate in and support PCI compliance initiatives.

Appendix 5: Glossary

Term	Definition
Altered Currency	Currency that has been changed or tampered with in order to attain a greater amount for the currency than its face value.
Bank Check	Check drawn by a bank on itself and signed by an authorized officer.
Bank Money Order	Check drawn by a bank on itself. The amount is encoded by the customer's bank, and the customer completes the rest of the check. There is always a maximum limit to the check amount.
Beginning Cash, Cash Drawer	Cash in the handler's drawer at the start of the day or shift. Drawer used to store currency, coins, and checks during cash handler's shift when completing transactions. This drawer should be locked when the cash handler is away for any reason.
Cash	Coin, paper currency, and all forms of negotiable instruments. Examples of negotiable instruments are personal checks, cashier's checks, bank drafts, traveler's checks, money orders, and credit card charge slips
Check	Draft or order on a bank to be drawn upon deposit of funds for payment of a certain sum of money to a person named or to a bear and payable on demand.
Cash Suspense Receipt	Kittitas County document that records revenue for a specific department.
Collusion	A secret agreement between two or more people to break a law.
Counterfeit	Currency or coins that have been fraudulently manufactured. Creating counterfeit money is a felony. Makers are subject to fines and imprisonment. To leave money with a bank or the Treasurer's Office for credit to a bank account or fund.
Deposits	Slip for which a depositor lists cash and items deposited.
Embezzlement	Fraud is committed when an employee steals or assists another to steal. Fraudulent misappropriation ions of money or property entrusted to one's care.
Ending Cash	Cash in a cash handler' s drawer at the end of the day or shift.
Endorsement	Signature placed on the back of a negotiable instrument according to law which transfers the instrument to another party.
Forgery Fraud	The alteration of documents or instruments with fraudulent intent. An attempt to obtain funds in other than appropriate and legal names.
Guaranty Deposit	Money deposited with the County Treasurer's Office and held in trust during a specific period of time. This money is refundable if not needed.
Hold	The restriction of payment or part or all of the funds in an account.

Identification	Information piece that guarantees that its holder is truly whom he or she claims to be and who is detailed on the information piece.
Loss	A cash handler obtains physical custody of money, and then, due to negligence, theft, or other reason, cannot deposit that money with the County Treasurer.
NSF-Non-Sufficient Funds	Checks returned by the bank due to insufficient funds, closed accounts, invalid signature, stop payment, or any other condition making the check invalid.
Overage	Amount by which cash or its equivalent exceeds the proper balance.
Over/Short Account	Specific account that departments can use to document when a deposit is over or short.
Payee Payer	Party to whom a check is payable, Party signing the check.
Petty Cash	A revolving fund for very limited purposes. They provide a given amount of cash on hand, the primary purpose being to provide change. Some petty cash funds are used for small expenditures and reimbursed by voucher.
Postdated Check	A check dated ahead. It is not payable until the date written on the check. This is not a legal document and should not be accepted.
Shortage	An intentional collection error made by the cash handler such as he/she did not obtain physical custody of money or a change-making error.
Stop Payment	Notification that a restriction has been placed on one's ability to cash a particular check. If a check has been lost or stolen, or if payment no longer should be made, a stop payment is initiated by the customer.
Transmittal - Cash Suspense	The form which is submitted to the County Treasurer for all monies (cash or checks) collected by a department or district.

Credit Card Glossary

Term	Definition
Address Verification Service (AVS)	A risk management tool that enables the County to verify the billing address of a customer presenting a credit/debit card for payment. An AVS request is included with the transaction authorization request. A code is returned by the Issuers indicating whether the address given by the cardholder matches the address in the Issuers file. A partial or no-match indicates a fraud risk.
Card Verification Value (CVV)	A unique value calculated from the data encoded on the magnetic strip on a credit/debit card, validating card information during the authorization process. The 3 digit, non-embossed number printed on the signature panel on the back of the card immediately following the last four digits of the credit/debit card account number. Issuer-Financial institution that issues credit/debit cards to cardholders and with which each cardholder has an agreement to repay the outstanding debt on the card.

Cardholder	The customer to whom a credit or debit card has been issued or the individual authorized to use the card.
Cardholder Data	All personally identifiable data about the cardholder (i.e., account number, expiration date, and cardholder name.)
Chargeback	A processed transaction that is later rejected by the customer and returned to the Acquirer.
Company	Management Accounting and Executive offices that approve all third-party service providers and coordinate the policies and procedures for accepting Credit and Debit cards at Kittitas County.
Credit Cards	A plastic card used to initiate a credit transaction for the purchase of goods and services.
Credit or Debit Card Account Change	Any change in the payment account including, but not limited to: the use of existing Credit or Debit card accounts for new purposes; the alternation of business processes that involve Credit or Debit card processing activities; the addition or alteration of payment systems; the addition or alternation of relationships with third-party Credit or Debit card service providers, and the addition or alternation of Credit or Debit card processing technologies.
Credit or Debit Card Industry (PCI) Data Security Standard (DSS)	A multi-faceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures.
Debit Cards	A plastic card used to initiate a debit transaction for the purchase of goods and services.
Encryption	The process of converting information into an unintelligible form to anyone except holders of a specific cryptographic key. The use of encryption protects information between the encryption process and the decryption process against unauthorized disclosure.
Kittitas County Management	A Kittitas County employee within a department who has primary authority and responsibility for Credit or Debit card and eCommerce transaction processing within that department.
Payment Card	Any Credit or Debit card/device that bears the logo of American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or VISA, Inc.
Receipt	A verification document to be printed duplicate and presented to the customer before credit card payment can be accepted.
Sensitive Authentication Data	Security-related information (card validation codes/values, full magnetic stripe data, or personal identification number (PIN)) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form.
Staff Employee	For the purposes of the PCI DSS and this policy, a Staff Employee is defined as entity that accepts Credit or Debit cards bearing the logos of any of the five members of the Payment Card Industry Security Standards Council (American Express, Discover, MasterCard or VISA) as payment for Kittitas County training and/or services.

Appendix 6: Internal Controls Checklist

**This form must be completed by the manager and submitted with the acknowledgment form(s).*

Question	Yes	No	N/A	Comments
Policies				
Have cashiers received training on how to properly handle cash and other types of payments received?				
Is there a formalized cash receipting policy? Is this reviewed with cashiers periodically?				
Do the policies or procedures require that cashiers accept only payments made by check or credit card for the exact amount of transaction?				
Do the policies or procedures prohibit the cashing of personal checks?				
Are cashiers required to take vacations and/or rotate job duties periodically?				
Start-up cash				
Is written authorization in place for the amount of start-up cash used?				
Is the start-up cash counted and verified when the cashiers receive their drawers at the beginning of a shift?				
Is the start-up cash kept in a secure location when not in use?				
Cash intake				
Are signs posted notifying customers to expect a receipt for every transaction?				
Are pre-numbered receipts issued (manual systems) or unique transaction numbers assigned (computerized systems) for all transactions, except possibly mailed-in payments?				
Do all receipts, whether generated manually or by computer, require the payment mode (such as cash or check or credit card) to be listed?				
Do cashiers immediately endorse checks "for deposit only" and date stamp them?				
Are collections secured throughout the day by use of registers or locking cash drawers?				
Is each cash drawer accessible to only one person — the custodian — even during breaks or lunches?				
Do cashiers lock their cash registers, cash boxes or receipting terminals when they step away?				

Are all payments receipted and recorded immediately, regardless of whether additional research is needed (such as where to code the payment)?				
Do cashiers balance their drawers at the end of each shift and record deposit overages or shortages?				
Does management monitor over/short activity to ensure such activity is reasonable and within normal ranges?				
Manual receipts				
Are manual receipt books kept in a secure location?				
Do manual receipt books identify the government's name? Note: rediform type receipt books should not be used.				
Are all manual receipt books tracked and accounted for, used and unused?				
If a manual receipt book is used, is the original voided or canceled receipt documentation kept and accounted for?				
Mailed payments				
Are mailed payments recorded on a remittance list as mail is opened?				
Do two people open the mailed payments together (one opens and the other records on the remittance list)? If this is not possible, proceed to next question.				
If two people do not open mailed payments, have you taken other steps to reduce your risk?				
Does someone independent of cash receipting match the remittance list to the deposit records?				
Money transfers				
If any cash or checks are transferred between staff, is there documentation and agreement between both people involved as to the amount of funds transferred? For example, this might occur if a deposit is consolidated.				
Cash registers				
Are all cash registers in good working order and capable of generating cash receipts?				
If the cash register cannot generate a receipt, is an official receipt book used instead?				
Does the cash register generate a record of its transactions that is used to verify transactions? (Note: this is commonly referred to as a Z tape.)				
Is the Z tape numbered sequentially, dated and time stamped?				

Does someone monitor Z tapes for a high number of "no sale" transactions, indicating the cash register is being opened without a transaction rung in?				
If managers use a cash register key to authorize a void, is the key secured at all times?				
Receipting software				
Do all cashiers have unique usernames and passwords, and do they sign in with these credentials when processing receipting transactions? Are these credentials kept secret and protected from use by others?				
Do cashiers have system access that is limited to only what they need to carry out their duties?				
Does someone independent of cash receipting control the user permissions in the receipting software?				
Does the system prevent cashiers from posting transactions to earlier or later periods? If not, is this monitored by management?				
Voids or adjustments				
If the cashier can perform voids or adjust transactions, is the reason documented and support retained?				
If cashiers can perform voids or adjust transactions, does management ensure it reviews all potential void or adjustment activity, such as by managers generating reports on their own?				
Refunds				
If cashiers can process refunds, is each transaction adequately documented, with information such as the reason for the return and the customer's information?				
If cashiers can process refunds, are those refunds authorized and reviewed by management?				
If cashiers can process refunds, does management ensure it reviews all potential refund activity, such as by managers generating reports on their own?				
Security				
Are cash and checks secured before deposit, such as in a safe or other locked location?				
Does the security provided for the deposit seem reasonable, given the amounts on hand? For example, it might not be appropriate to store large sums in a locking file cabinet. Instead, such amounts of stored cash might justify a camera system.				

Is the deposit kept locked up at all times when unattended? For example, is the safe door actually closed, requiring a code or combination to be entered to access it?				
Are keys or safe combinations to access funds given only to those who absolutely need access?				
When employees leave, is the safe combination changed or does someone ensure the keys are returned?				
If keys are used to access the deposit, do senior personnel maintain a list of who has them, and are all keys safeguarded?				
If a safe is used, do senior personnel maintain a list of who has access to the safe?				
Bank deposits				
Does the preparer of the deposit initial their work?				
Are all funds deposited in full? This means monies received are directly deposited and not used to pay bills or fund petty cash.				
Do the deposit slips indicate the cash and check subtotals for the deposit, as well as the amount of each check?				
Are secure transfer bags (sealed or locking) used to transport deposits to the cashier or bank?				
If locking bank bags are in use, are the keys secured at all times?				
If tamper proof (sealed) bank bags are used, are they pre-numbered and numerically accounted for (both the used and unused bags)?				
Are deposits made as frequently as expected to comply with legal and policy requirements? If they are not done in 24 hours, do you have an approved waiver?				
If deposits are not done in 24 hours, when was deposit frequency last evaluated? Does it make sense in light of the volume of cash activity at the receipting location?				
If the deposit is made with a financial institution (as compared to the County Treasurer), is it a qualified depository (RCW 39.58)?				
Does a manager periodically perform a "last look" at the deposit?				
NSF checks				
If those who receipt payments also handle the NSF checks returned by the bank, does management monitor this activity to ensure activity is valid and appropriate?				

Cashiers have customer account duties				
If those who receipt payments also can adjust customer account balances, does management periodically review this adjustment activity to ensure it is valid? Does management ensure it reviews all adjustments, such as by managers running reports themselves?				
If those who receipt payments also invoice customers, does management monitor to ensure billing is done at appropriate amounts?				
If those who receipt payments also apply payments to customer accounts, does management monitor that payments are posted to the correct accounts?				
If those who receipt payments also apply payments to customer accounts, does management monitor that the total amount collected agrees to the total payments applied to customer accounts?				
Reconcile the deposit				
Is the person performing the reconciliation independent of cash receipting?				
Is the reconciliation performed promptly after the deposit is made?				
In performing the deposit reconciliation, is the deposit reconciled by comparing the validated bank receipt to the deposit slip, as well as to ALL underlying receipt records or system reports?				
In performing the deposit reconciliation, are all prenumbered receipts accounted for?				
In performing the deposit reconciliation, are cash and check subtotals compared between the source records and deposit records?				
Is there a policy or procedure for following up on discrepancies and notifying other key individuals in the organization?				
Additional reconciliation				
Is the suspense fund reconciled monthly and any outstanding items researched and resolved?				
Does an independent person reconcile the bank statement and ensure all deposits in entity records agree to the bank's information?				
Additional oversight				
Does someone independent monitor that deposit activity is reasonable and matches expectations?				

Does someone independent periodically perform surprise cash counts of cash drawers?				
Does someone monitor unanticipated revenues?				
Credit cards				
Are employees trained to know how to properly handle a credit card transaction?				
Does someone independent reconcile credit card receipts to the total payment activity shown in entity records? Is it done daily?				
Does someone independent reconcile daily activity to the amount reflected on the monthly bank statement?				
If employees can process credit card refunds or credits, are adequate controls or oversight in place to ensure each is valid?				

Source

This resource has been developed by the Center for Government Innovation of the Office of the Washington State Auditor. Please send any questions, comments, or suggestions to Center@sao.wa.gov.

Disclaimer

This resource is for informational purposes only. It does not represent prescriptive guidance, legal advice, an audit recommendation, or audit assurance. It does not relieve governments of their responsibilities to assess risks, design appropriate controls, and make management decisions.

Appendix 7: Acknowledgment Form – Cash Management

EMPLOYEE ACKNOWLEDGEMENT

As an employee of Kittitas County, I understand that the collection and handling of cash is a responsibility of my job.

I understand that I am personally responsible for all County money within my control, and may be held liable for any loss occurring, unless the loss is caused by an act of God, a robbery, or a statutory exception.

I understand that any cash overage or shortage must be reported to my elected official/Department Head.

I acknowledge that a discrepancy of \$50 or larger, either over or short, will result in a notification being sent to the auditor's office, a record placed in my personnel file, and the possibility of a written reprimand.

I have read, understand, and agree to abide by the Kittitas County Cash Handling Policy.

Name (Print):

Signature:

Department:

Manager/Supervisor:

Date:

Appendix 8: Credit Card Policy Acknowledgment Form

I acknowledge that I have received, read, and understand the content of the Kittitas County Credit Card Policy. I understand that adherence to this policy is essential for maintaining the security and confidentiality of credit card information and ensuring compliance with relevant regulations.

By signing this acknowledgment form, I commit to complying with the provisions outlined in the Credit Card Policy document. I am aware of the responsibilities associated with handling credit card information and the importance of safeguarding this sensitive data.

I have read, understand, and agree to abide by the Kittitas County Credit Card Policy.

Name (Print):

Signature:

Department:

Manager/Supervisor:

Date:

