MULTNOMAH COUNTY

CASH HANDLING MANUAL

Prepared by Multnomah County Treasury
501 SE Hawthorne Blvd. Suite 531
Portland OR 97214
Phone: 503-988-3681, 503-988-3440, 503-988-5535
Fax: 503-988-3292
treasury@multco.us

Updated October 2018

Table of Contents

CHAPTER 1 – Multnomah County Treasury

Treasury manages the County's cash assets, investment portfolio, debt, banking services and relationships, and broker/dealer relationships, as well as providing responsive and pro-active customer support and service internally and externally. Treasury clears and balances bank deposits consisting of payments for property taxes, excise taxes, and turnovers from other government entities. Treasury processes and transfers bank data, processes and balances incoming electronic funds transfers and initiates outgoing funds transfers. Treasury manages more than 60 separate individual fiduciary trust accounts per statutory mandate.

Treasury function is guided by and in pursuant to the fiscal management policy of Multnomah County:

- To preserve capital through prudent banking and cash management activities
- To achieve the most productive use of cash, minimize operating cost and to control receipts and disbursements
- To maintain competitive and good working relations with financial institutions
- To ensure that all financial systems, functions and controls meet generally accepted auditing standards
- To provide safety to employees

PURPOSE

Multnomah County Treasury is responsible for all cash handling in the County. However, departments have primary responsibility for implementing good cash controls and work together with Treasury. Treasury manages all banking relationships and reports directly to the Chief Financial Officer.

Treasury standards are measured in terms of three broad areas, accuracy, accountability and security. Accuracy of cash handling, depository and reconciliation functions, accountability for transactions cash handlers perform with clear audit trail for all cash activities and ensuring departmental operational cash procedures have security aspects built in for the safety of cash handlers and county assets.

CHAPTER 2 – Currency, Coins and Checks

Treasury developed this cash handling training manual as reference tool for proper cash handling techniques. The basis of all cash handling rules in Multnomah County are the policies and procedures highlighted in FIN administrative procedures FIN-3, FIN-4, FIN-5, FIN-6, FIN-19.

The purpose of this manual is to establish general standard for all County employees who collect and handle cash as part of their job.

In general, funds collected by county employees are considered "public funds" as defined by the Oregon Revised Statutes. As a Multnomah County cash handler you have the custodial responsibility for the proper handling of public funds. Detailed procedure is listed in FIN-6 which governs the handling of funds by an agent of the county. For this procedure, an agent is defined as any individual on the County payroll or person having a contractual agreement with the County.

CURRENCY & COINS

Recognizing currency

The Federal Reserve Bank of 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 bearing a portrait of a different famous American.

Denomination	Portrait
$1.00	George Washington
$2.00	Thomas Jefferson
$5.00	Abraham Lincoln
$10.00	Alexander Hamilton
$20.00	Andrew Jackson
$50.00	Ulysses S. Grant
$100.00	Benjamin Franklin

Recognizing coin

The United States Mint is responsible for coin production. Philadelphia and Denver are the two remaining mints still in production in the United States. Today six kinds of U.S coins are issued.

Value	Name	Composition
$0.01	Penny	Copper Plated Zinc
$0.05	Nickel	Cupro-Nickel
$0.10	Dime	Cupro-Nickel
$0.25	Quarter	Cupro-Nickel
$0.50	Half dollar	Cupro-Nickel
$1.00	Silver Dollar	Silver
$1.00	Susan B. Anthony Dollar (1979-81, 1999)	Cupro-Nickel
$1.00	Sacagawea Golden Dollar (2000)	Manganese-Brass
$1.00	Presidential $1 Coin (2007 – 2011)	Manganese-Brass
$1.00	Native American $1 Coin (2009 - present)	Manganese-Brass

COUNTING CURRENCY & COIN

There are two common ways of counting currency, hand to hand and hand to table method. The hand to table method is the preferred method to use to reduce errors. Cash handlers should establish a set, comfortable routine for counting money.

Counting Currency: Hand to Hand Method

1. Separate bills into denominations with all the bills face up
2. Stack the pile in order with the lowest denomination on bottom and the largest denomination on the top
3. If the pile contains more than one denomination, count the largest denomination first
4. Place the pile on one hand
5. Transfer one bill at a time from one hand to your other hand as you count
6. Check each bill, as you count to ensure correct denomination
7. If your totals do not agree, repeat the count until they do

Counting Currency: Hand to Table Method

This method is the same as the hand to hand method except that instead of placing the currency in your hand you will place it on the table as you count. This allows you to see the bills more fully to check for raised notes, and also helps to ensure you do not have more than one bills stuck together.

Counting Coin

As with counting currency, establishing a set routine for counting coins can ensure accuracy as a cash handler. When accepting rolled coins, ensure the contents are matching the declared amount for accuracy. Coins are stored in coin wrappers or rolls, to ensure accurate handling. Each person counting and inserting the coins into wrappers should initial and date the wrappers. When you open the wrapper of coins, always empty the whole package into the coin drawer or coin machine. Have customers who pay with rolled coins put their names, address and daytime telephone number on the outside.

Remember

- Always keep money received and count in view of the customer
- Never place money received in cash drawer before the transaction is complete
- Separate the currency from coins
- Count the currency before the coins
- Count each currency denomination separately
- Separate coins in denominations
- Count each coin denomination separately
- Count all currency and coin in the presence of the customer
- Verify the grand total against the amount listed on the billing or the invoice
- If any discrepancies exist between your total and the customer's total, count the money again. If the discrepancy still exists, ask a co-worker to count the money.
- Put away currency and coins from the last transaction before starting a new transaction.

MAKING CHANGE

To ensure the accuracy of all transactions, it is important that the cash handler follow a routine, accepted practice of making change. There are two ways to give change back to a customer

1. The cash register automatically calculates the dollar amount to be returned to the customer
2. The cash handler counts from the amount of sale to the amount tendered. Change should be counted at least two times; once when the cash handler counts it out of the cash drawer and a second time when the cash handler counts it back to the customer. Hopefully a third time when the customer counts it along with the cash handler.

Always give the customer a receipt and put the amount received in the cash drawer and close the drawer.

STRAPPING & BUNDLING CURRENCY

Your job as a cash handler includes removing from circulation all torn or otherwise mutilated bills. A cash handler may ask for another bill if a customer offers a mutilated

bill. However, if the customer cannot substitute the bill, the cash handler should accept the mutilated bill if it is legal. Whenever you receive such a bill, place it aside in your cash drawer to return to the Treasury with your deposit. Do not give mutilated currency or coin as change to other customers.

Currency is mutilated whenever it is torn, written on, missing a portion or otherwise damaged. Coins are mutilated whenever they are bent, worn, broken or otherwise damaged. If the bill is more then 3/5 (60%) intact (or ¾ of the two serial numbers), the bank will pay its face value. If the bill is less than 2/5 intact, the bank will not honor its value.

COUNTERFEIT CURRENCY

Counterfeit notes (counterfeit bills and coins) are prevalent in any environment where money is exchanged. Multnomah County is also vulnerable to receive these and hence we have the responsibility to report it to United States Secret Service if we come across in course of business.

However, best cash handling practices help us detect these by examining them carefully, using counterfeit marking pens and taking time to process transactions as the consequence is we lose money if it turns out to be counterfeit after it is accepted from the customer and processed for deposit.

Visit the United States Secret Service website section 'Know Your Money' for detailed explanation of various aspects of counterfeit currency and coins detection, https://www.secretservice.gov/data/KnowYourMoney.pdf

What to do if you receive a Counterfeit

1. Identify the note received is counterfeit by using counterfeit bill detector pens
    a. Mark a dot or a line anywhere on the bill
    b. Wait about 5 seconds for the detector to check for any reaction
    c. If it turns yellow, it means the money is genuine. If it turns black, the money is suspect counterfeit
        i. the yellow coloring on the genuine bill will disappear after few seconds
        ii. the black mark will remain until the bill is destroyed
2. Notify your supervisor / manager on site immediately
3. Contact building security if need be. Let the dispatcher know your situation and request back up if need be. Be prepared to provide descriptions of the passer, any companions, and license plate numbers of any vehicles used if possible
4. Do not return the note to the passer. If the passer becomes aggressive and demands the note back, give it back. Maintaining your personal safety is more important than identifying a potentially counterfeit note
5. Delay the passer if possible. If the passer decides to leave, do not try to stop them

6. Limit handling of the note.
    a. Write your initials and date in the white border areas of the suspect note
    b. Carefully place it in a protective covering, such as an envelope
7. Supervisor / manager needs to contact local Secret Service office at 503-326-2162
8. Supervisor / manager needs to complete form SSF 1604 USSS Counterfeit Note Report (PDF)
    a. Submit it to the local secret service jurisdictional field office 805 SW Broadway, Suite 520, Portland, OR 97205
    b. Make three copies of the form SSF 1604, send two to Secret Service Field office and keep on file at site. If you are making copies of the bills / notes for record purposes please remember to make it much larger than the normal size otherwise it will be counterfeit.
    c. Secret Service will return one form as an acknowledgement of receipt
    d. It is very important to call Secret Service local office if the form details are not clear. They want us to make sure all the required information is accurately filled out to avoid processing delays
    e. We should hear back in within 3-4 weeks during non-holiday months and 6-7 weeks during holidays.

What to do if currency deposited is notified by bank as being suspect counterfeit

1. Bank will post debit adjustment for the suspect counterfeit note amount
2. Departments need to post credit memo to record the debit adjustment
3. Suspect counterfeit notes discovered by bank's cash services are considered suspect counterfeit notes until confirmed by the U.S. Secret Service (USSS)
4. All suspect counterfeit notes are required by federal law to be turned over to the USSS
5. Depending on volume of transactions on the day this item was collected, possibility of identifying the transaction to a client, management need to come up with a plan of action to post this debit adjustment in SAP and possibly follow up
6. Bank will be notified by secret service after determination is made on the suspect currency
7. If it is not counterfeit then we will see bank credit adjustment and departments will make entries to offset the credit memo.

Should you have any questions please email treasury@multco.us

ACCCEPTING CHECKS

Checks as Negotiable Instruments

A check is a negotiable instrument that is drawn on a bank and payable on demand. The "drawer" or "maker" of the check is the party issuing and signing the check. The drawer may be one or more individuals acting on their own behalf, or the drawer may be one or more individuals authorized to act on behalf of a company, corporation, partnership or government agency. The "drawee" is the party on whom the check is drawn, usually a bank or trust company. They are the party that will pay the check upon presentation by the payee.

By taking a check you are accepting the makers promise to pay. The promise to pay is all the county has until the check is presented, by deposit, to the bank for payment. Until that check is cashed, the funds are credited to the county accounts, it is only a promise of funds. Checks should never be cashed, or allowed to be written for more than the sale amount**. Do not cash checks for employees or the public, it is an unauthorized and generally illegal loan of public funds**.

Parts of a Check

There are seven basic requirements a check should have in order to be presented for payment. Before accepting a check from a customer, you should verify that the check has all of these elements.

1. **Current Date**: The check must have a current date. While a check dated with yesterdays date is acceptable do not accept "stale" or "post" dated checks. A stale check is dated 180 or more days (limits vary) in the past and the postdated check is a check dated in the future. If a customer puts the incorrect date on the check, have them change the date and initial the correction. ***To reduce the incidence of NSF (non sufficient funds) checks, all checks should be deposited within 24 hours of being received from a customer. Banks deposits should be made daily. See FIN-6.***
2. **Payee**: The check must have a payee, which is the company or individual being paid for goods and services. Only accept checks made payable to Multnomah County or the name of your department.
3. **Payor**: The check must have payor, which is the company or the individual paying for good or services. The name and address of the payor should be pre-printed on the front of the check however this is not a mandatory requirement for negotiability or acceptance of the check.
4. **Dollar Amount**: The dollar amount must appear twice. It must be both spelled out and printed numerically. If discrepancy between the written and numeric amount occurs, the bank goes by the legal amount which is the spelled amount.
5. **Bank**: The check must be drawn on a bank whose name appears on the check.
6. **Signature**: The check must be signed by the payor or drawer.

7. **MICR numbers**: Magnetic Ink Character Recognition (MICR) numbers are printed at the bottom, left hand corner of the check. If not, the check will require special handling. The MICR line numbers are very important elements to the normal processing of the check. They allow the bank's routing identification, the customer's account number, the check number, and often the check amount to be read automatically by bank's processing equipment very rapidly and accurately. If these numbers do not appear, the check will not be processed correctly.

Other Types of Checks

Cashier's checks

This is a check drawn by a financial institution on its own funds, usually purchased by the bank's customer. Since only the failure of the bank would cause the financial institution not to honor such checks, they are accepted almost as readily as currency. Caution should still be exercised, as fraudulent cashier's checks can be produced. No cash may be given for any check transaction.

Personal Money Order

A personal money order is check purchased by a customer from a vendor for currency or against bank balance. When issued, it shows a drawee bank and an amount. The purchaser fills in the date, the payor and the payees name and address. Financial institutions usually restrict the maximum amount for which they issue a money order. The amount is usually printed on the face of the money order. Check the money order for the words, "Not to exceed $---." Money orders are accepted almost as readily as currency, but caution should be exercised, as fraudulent money orders can be produced and the accounts on which the money orders are drawn can be insufficient. Money orders may begin to decline in value at some point so the issue date on money order should be current. No cash may be given for any check transaction.

Traveler's checks

These checks are designed for use by persons on business or vacation trips, but are also used in other situations. They are signed on the face of the check when purchased and countersigned when negotiated, either on the face or on the back. When using traveler's check at a county facility, the customer must countersign and write in the payee in the presence of a county cash handler. Traveler's checks should be stamped with the county endorsement and place with other checks. The county cannot accept traveler's checks drawn on foreign currencies. County cash handlers should ask for proof of identification when taking traveler's checks. Change from a purchase may be given back when a customer pays by traveler's checks.

Check endorsements

All checks should be endorsed upon receipt either with a stamp or manually. Treasury will assist all county departments with all banking supplies including endorsement stamps. The endorsement language can vary between departments, but generally include "For deposit only, Multnomah County – Department / Office"

In accordance with federal law, the endorsement must be stamped in the first 1.5 inches on the back of the check on the trailing edges. The remainder of the back of the check must be left blank. It is important to endorse checks to the County as soon as possible, to reduce the possibility of their being deposited to the account of another party.

Checks Frauds

Check fraud is one of the biggest challenges facing businesses and financial institutions today and it is estimated that the annual losses due to check fraud run into billions of dollars. As you can imagine with the advancement in technology it is becoming increasingly easy for criminals to manipulate checks.

A large amount of check fraud is due to counterfeiting through desktop publishing and copying to create or duplicate actual documents (checks), which consists of removing some or all of the information and manipulating it to the benefit of the criminal.

Some of the common types of check fraud are forgery, counterfeiting and alteration, paperhanging (purposely writing checks on closed accounts), check kiting (opening accounts at two or more financial institutions and using the float time of available funds to create fraudulent balances)

What are the signs of bad checks?

- The check lacks perforation
- The check number is missing
- The check number is low (like 101 up to 400) on personal checks or (1001 up to 1500) on business checks
- The customer address is missing
- The address of the bank is missing
- Addition to the check (i.e. phone number) is writing by hand
- The type of font used to print the customer's name looks visibly different from the font used to print the address.
- There are stains or discoloration on the check possibly caused by alterations
- The MICR is shiny, as the real magnetic ink is dull and non-glossy in appearance
- The MICR number is missing
- The name of the payee appears to have been printed by a typewriter
- The check lacks an authorized signature

Preventive measures

- Store checks, deposit slips, bank statements and cancelled checks in a secure locked location
- Never leave check book in the vehicle or out in the open
- Reconcile bank accounts every month and notify any discrepancies in within 30 days otherwise you may become liable for any losses due to check fraud
- Never give your account number to someone you don't know, especially over the phone
- When you receive your check order, make sure all the checks are there and that none are missing. Report missing checks to your bank at once or if you don't receive you order in within the reasonable mail time, notify bank immediately

Please email treasury@multco.us with any questions.

CHAPTER 3 - CREDIT CARDS, PCI POLICY & GUIDELINES

ACCEPTING CREDIT CARDS

We all have seen a substantial increase in the usage of credit cards as a means of payment for goods and services in recent times. By all accounts the numbers and spread of usage is growing much faster which has the benefits of reduced fraud potential and increased customer convenience. However, credit card frauds have also increased substantially which has necessitated the Payment Card Industry to come up with strict rules, standards and guidelines for merchants and businesses to comply with.

Multnomah County accepts payment by credit card in all its major areas of operation through swipe machines and online payments. All new merchant bank accounts are approved by CFO after review by Treasury. All merchant bankcard communication, such as PCI compliance processes, chargeback's, product integration with Departments, supplies, opening and closing of accounts must be coordinated through Treasury.

Things to remember for desk operational procedures

- All face-to-face transactions should have the payment card present and obtain a signature with the exception of the dollar limit no signature card program Multnomah County participates in. Always verify that the card is valid and signed. Compare signatures and check for ID.
- If it is not a face-to-face transaction, some other method must be used for securing the payment (i.e. mail in form with credit card information and signature, fax in signature, etc.). Request a signed authorization letter and obtain a signature of the cardholder.
- Merchant locations may accept card numbers via phone, fax, and U.S. mail. NEVER ASK FOR CARD INFORMATION OR SOLICIT CARD INFORMATION VIA E-MAIL.
- Merchants must keep all card numbers and information secure and confidential.

- Sensitive card information (full account number, type, expiration date, card validation code or track data) must NEVER be stored on any computer, database or server.
- Multnomah County merchants locations will never agree to disclose or acquire any information concerning a cardholder's account without the cardholder's consent. Multnomah County Departments will not sell, purchase, provide, disclose or exchange card account information or any other transaction information.
- Merchants will keep an original copy and follow the retention schedule. All card documentation containing card account numbers must be maintained in a secure environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked office, and safes. Credit card receipts should typically be treated the same as you would treat large sums of cash. Your department will be responsible for any losses due to poor internal controls.
- A cash advance or withdrawal from your department to a cardholder, or to yourself, is not authorized. Merchants may not accept money from a cardholder and subsequently prepare a credit draft for the purpose of creating a credit to the purchaser's account. The terminal may only be used for transactions related to purchases of Multnomah County goods and services.
- Merchants agree that the sales draft represents a bona fide, newly created transaction involving the merchandise and/or services itemized on the sales draft. A customer should not be charged before merchandise is shipped. In the case of an intangible product (i.e. Registration) process the charge to the customer when registration confirmation is sent.
- Merchants are required, in good faith, to maintain a fair policy for the exchange and return of merchandise and for resolving disputes over merchandise and/or services purchased with a payment card. If a transaction is for non-returnable, non-refundable merchandise, this must be indicated on all copies of the sales draft before the cardholder signs it. A copy of your return policy must be displayed in public view.
- Merchants will give proper credit for returns and adjustments by performing the proper function on the terminal. Under no circumstances should any card refund or adjustment be paid to a cardholder in cash. If cash is refunded and the cardholder files a dispute, your department will bear the loss of income from the transaction.
- All fees associated with processing of credit card transactions will be paid by the department.

ROLES

Credit Card Handling Supervisor

- Design an adequate process and procedure to ensure the following standards are maintained:
- Keep secure and confidential all cardholder numbers and information. Credit card receipts should typically be treated the same as you would treat large sums of cash. The department will be responsible for any losses due to poor internal or inadequate controls.
- Sensitive cardholder data (i.e., full account number, type, expiration, and track (CVC2/CVV2) data), cannot be stored in any fashion on computers or networks.
- Credit card numbers must not be transmitted in an insecure manner, such as by e-mail, unsecured fax, or through inter office mail
- All documentation containing card account numbers must be maintained in a "secure" environment limited to dependable, trustworthy and accountable staff. Secure environments include locked drawers, file cabinets in locked offices, and safes.
- All documentation containing card account numbers must be secured and follow the Multnomah County retention schedule.
- Restrict access to credit card data and processing to appropriate and authorized personnel.
- Background checks must be performed prior to hiring of any positions with unrestricted access to cardholder information
- Establish appropriate segregation of duties between credit card processing, the processing of refunds, and the reconciliation function. Supervisory approval of all card refunds is required.
- Perform an annual self-assessment to ensure compliance with this policy and associated procedures in conjunction with Treasury, IT security for the overall PCI compliance.
- Notify Multnomah County Treasury and IT prior to implementation of any technology changes affecting transactions processing associated with the merchant account.
- Departments should periodically inspect the credit card terminal devices to look for tampering or substitution and report any suspicious behavior of the devices being tampered with to Treasury right away. It is also very important to verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to troubleshoot devices.

Treasury Manager

- Review and approve the establishment of new merchant credit card accounts, change type of account or close a merchant account
- Administer the process of obtaining new merchant numbers. Conduct periodic reviews of existing merchants regarding safeguarding and storage of cardholder

information. Provide periodic training on the secure storage and disposal of all non-ecommerce credit card paper transaction records in conjunction with cash handling training.

- Ensure PCI compliance with regard to all the merchant accounts owned by Multnomah County. Coordinate with IT security by hiring external scan vendors to perform quarterly scans and annual penetration tests of our system.
- Review and approve implementation of any technology changes and payment gateways associated with credit card transactions processing.
- Treasury will book monthly expenses for the merchant accounts, follow up with SAP entries by departments for bank reconciliation and help resolve chargeback issues.

MULTNOMAH COUNTY – POLICY STATEMENT

Payment Card Industry Data Security Standard (PCI DSS)

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted in accordance with the standards and procedures listed in the Related Documents section of this Policy (See Attachment I). No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

This policy shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

Applicability and Availability

This policy applies to all employees of Multnomah County and where relevant to vendors, contractors, and business partners of Multnomah County

Policy Requirements

Configuration standards maintained for applications, network components and critical servers. Procedures for cardholder data handling, retention and disposal must be maintained by each department in line with the County's retention schedule. Credit card numbers must be masked when displaying cardholder data. Unencrypted Primary Account Numbers may not be sent via email. Procedures for cardholder data control must be maintained by each department and must incorporate access rights to privileged User IDs necessary to perform job responsibilities and assignment based on individual personnel's job classification and function.

Multnomah County's Human Resources Policies and Procedures relating to Personnel Rules, Administrative Procedures and Executive Rules such as 'Use of Information Technology – Personnel Rule 3-35' and 'Employee Responsibilities - Personnel Rule 3-10' is applicable where relevant.

Treasury in conjunction with Departments and IT will review risk assessments that identifies threats and vulnerabilities periodically.

Treasury will ensure service providers with whom cardholder information is shared, contracts require adherence to PCI-DSS by the service provider and contracts include acknowledgement or responsibility for the security of cardholder data by the service provider.

Notify by email at treasury@multco.us or call 503-988-3681 / 503-988-7441 / 503-988-5535 immediately with discovery of any incidence of data compromise.

MULTNOMAH COUNTY PCI COMPLIANCE

Frequently Asked Questions about PCI

What is PCI?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. Essentially any merchant that has a Merchant ID (MID).

The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC (www.pcisecuritystandards.org), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.). The payment brands and acquirers are responsible for enforcing compliance, not the PCI council.

Essentially there are three components:

1. PCI (Payment card industry) security standard council develops standards
2. Visa / MasterCard and other card companies establishes compliance requirements
3. Banks / Financial institutions called 'acquirers' enforce requirements on merchants

PCI Data Security Standards Requirements "Digital Dozen:"

Build and maintain a Secure Network

Requirement 1:	Install and maintain a firewall configuration to protect data
Requirement 2:	Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3:	Protect stored data
Requirement 4:	Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

Requirement 5:	Use and regularly update anti-virus software
Requirement 6:	Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7:	Restrict access to data by business need-to-know
Requirement 8:	Assign a unique ID to each person with computer access
Requirement 9:	Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10:	Track and monitor all access to network resources and cardholder data
Requirement 11:	Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12:	Maintain a policy that addresses information security

How many Merchant Accounts does Multnomah County currently have?

55 across 8 departments
4 through Official payments Corporation (property tax processing account OPC)

To whom does the PCI apply?

PCI applies to all organizations or merchants, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. Said another way, if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.

What are the PCI compliance 'levels' and how are they determined?

All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ('DBA'). In cases where a merchant corporation has more than one DBA, Visa acquirers must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, acquirers will continue to consider the DBA's individual transaction volume to determine the validation level.
Merchant levels as defined by Visa:

Merchant Level	Description
1	Any merchant -- regardless of acceptance channel -- processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant -- regardless of acceptance channel -- processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants -- regardless of acceptance channel -- processing up to 1M Visa transactions per year.

What level is Multnomah County at?

Currently at Level 3

What are the PCI compliance deadlines?

Any merchant that stores, processes or transmits cardholder data must be compliant now. Validation requirements for level 2-4 merchants are:

f.1 complete and validate an annual PCI self-assessment questionnaire
f.2 complete quarterly network scans to check systems for vulnerabilities
f.3 complete annual penetration testing to test that that your systems are hacker resistant
f.4 ensure that these security scans are performed by a qualified independent scan vendor

What are the penalties for noncompliance?

The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine on downstream till it eventually hits the merchant. Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can catastrophic to a small business.

What is defined as 'cardholder data'?

Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

Can the full credit card number be printed on the consumer's copy of the receipt?

PCI DSS requirement 3.3 states "Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)." However, we require departments to mask PAN to reflect only the last four digits on all printed receipts and reports.

Do I need vulnerability scanning to validate compliance?

If you electronically store cardholder data, post authorization or if your processing systems have any internet connectivity, a quarterly scan by a PCI SSC Approved Scanning Vendor (ASV) is required.

What is a network security scan?

A network security scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network. As provided by an Approved Scanning Vendors (ASV's) such as ControlScan the tool will not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

Note, typically only merchants with external facing IP address are required to have passing quarterly scans to validate PCI compliance. This is usually merchants completing the SAQ C or D version.

How often do I have to scan?

Every 90 days/once per quarter you are required to submit a passing scan. Merchants and service providers should submit compliance documentation (successful scan reports) according to the timetable determined by their acquirer. Scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV). ControlScan is a PCI Approved Scanning Vendor.

What if a merchant refuses to cooperate?

PCI is not, in itself, a law. The standard was created by the major card brands such as Visa, MasterCard, Discover, AMEX, and JCB. At their acquirers/service providers discretion, merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc., should a breach event occur. For a little upfront effort and cost to comply with PCI, we greatly help reduce our risk from facing these extremely unpleasant and costly consequences

Protect Cardholder Data

Cardholder data is personally identifiable information about a cardholder provided through use of a card such as card account number, cardholder name, card validation value or code , card expiration date, service code, and card magnetic stripe data. Storing, processing, or transmitting the account number is the critical component that makes PCI DSS applicable.

1. Do not store the full contents of any track from the magnetic strip (located on the back of a card, contained in a chip or elsewhere)
    a. ***NEVER store the card verification code or value or PIN verification value data elements*.**
2. Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card not-present transactions. It is never acceptable for merchants or service providers to retain CVV2 (Card Verification Value 2 Code) and CVC2 (Card Validation Code 2), data which consists of the last three digits printed on the signature panel of all Visa and MasterCard cards, in any manner for any purpose whether encrypted or unencrypted.
3. Do not store the personal identification number (PIN) or the encrypted PIN block.
4. Is the PAN (primary account number) masked when displayed? (the last four digits are the maximum number of digits to be displayed)
5. None of the printed copies (sales draft, merchant copy and batch settlement) should be mailed interoffice unless sent by secured courier and follow the County deposit retention schedule. The printed sales document should be kept in a locking file cabinet for audit with limited access.
6. Operations supervisor monitor closely to detect sending of any unencrypted PANS by end-user messaging technologies (ex. E-mail, instant messaging, chat), guard against skimming or any activity that would compromise cardholder data.
7. Acceptance of payment over phone at relevant locations should shred cardholder data immediately after completion of the transaction if noted.
8. Restrict access to cardholder data
    a. Access to system components and cardholder data should be limited to only those individuals whose job requires such access.
    b. All paper and electronic media that contain cardholder data are physically secure
    c. Develop procedures to help all personnel easily distinguish between employees and visitors, especially where cardholder data is accessible
    d. Proper authorization before entering areas where cardholder data is processed or maintained.
    e. Maintain strict control over the storage and accessibility of media that contains cardholder data

Compliance and Validation

Treasury will be the central point keeping track of compliance and validation process.

- Annual compliance and validation audit will be carried out by treasury with the departments
- Requirements for merchant account compliance whether individually or aggregated will be notified by treasury to respective departments
- Separate SAQ questionnaires will be maintained accordingly by Treasury in consultation with the departments and IT
- Costs pertaining to hiring services of external scan vendors will be shared by all users (departments)
- We will get annual compliance certificate from third party service providers to ensure they are compliant.

Policies & Procedures (See Multnomah County Policy)

- These guidelines along with relevant administrative procedures should be the basis of training staff and supervisors
- All correspondence relating to the merchant services will be handled centrally by Treasury in consultation with the department managers/supervisor
- Correspondence relating to any aspects of merchant account should be forwarded to department manager and Treasury
- Each department should frame operating procedures incorporating all aspects of compliance requirements mentioned above and contact treasury if assistance is required.

Merchant Resources

https://merch.bankofamerica.com/
https://www.pcisecuritystandards.org/
https://www.mastercard.us/en-us/merchants/get-support/security-training.html
https://usa.visa.com/visa-everywhere/security.html#2

CHAPTER 4 – SECURITY POINTERS

The following guidelines are provided to help ensure staff safety and minimize loss to Multnomah County;

- Unnecessary risks should never be taken. Cooperate with the robber.
- Avoid any confrontation and facilitate a rapid departure.
- Stay as calm as possible. Take no risks.
- Try not to panic or show any signs of anger or confusion.
- Make a mental note of any descriptive features or distinguishing marks on the robber, such as his/her clothing, hair color, eye color, scars, tattoos, etc.
- Touch nothing in areas where robbers were and note specific objects touched by robbers.
- Only if it is safe observe the direction the robber took.
- If possible, observe color and make of vehicle leaving the scene.
- Departments having security alarms should trip the alarm as soon as it is safe.
- 911 should be called as soon as it is safe.
- The robbery should not be discussed with anyone until the police arrive.
- The victim should, above all else, remain calm and try to remember the details. Write them down.
- Remembering physical characteristics of suspicious persons or assailants can greatly assist Police in their apprehension. Please fill out the robbery identification card immediately.

CONTACT POLICE, TREASURY (503-988-3681) & RISK MANAGEMENT (503-988-5851) AS QUICKLY AS POSSIBLE AFTER DEPARTURE OF SUSPECT(S)

CHAPTER 5 – SEGREGATION OF DUTIES

There **must** be a separation of duties between the person receiving *cash* and the person responsible for maintaining the accounting records. Cash receipt activity must be reconciled to the General Ledger monthly. The reconciliation must be reviewed by someone independent of the *cash* handling or recording functions (i.e., a supervisor or manager).

The following responsibilities should be distributed among personnel so that one person does not perform more than one:

- Opening mail, if applicable
- Receipting funds and endorsing checks
- Authorizing voids, corrections or debit entries
- Preparing deposits
- Reconciling to *General Ledger*
- Billing and collection duties

Only the minimum number of employees should handle *cash* from receipt to deposit. If the size of the departmental staff makes proper segregation of duties impossible, a second person must verify *reconciliations* of *cash* item accounts.

In general, the authorization, accounting/reconciling and the *cash* custody functions should be separated among employees. When these functions cannot be separated, a detailed supervisory review of related activities is required as a compensating control activity.

Departments are responsible for complying with the policies and procedures outlined in the administrative rules for developing detailed written departmental operating procedures. Treasury is available for consultation and review of departmental procedures. Departments are responsible for training designated employees in fund handling policies and procedures. Department supervisors/managers are responsible for the safekeeping of money that is received by their department and the prompt transfer of these funds to the
Bank.

Example of three person cash handling operation:

Roles	Receiving (handling) cash etc.	Preparing deposit	Reconciling receipts & deposits	Recording deposits to GL	Making cash deposits	Comparing deposits to GL entries
Individual1 Cash handler, Custodian	X				X	
Individual2, Alternate custodian		X				
Individual 3 Account Supervisor, Reconciler, Department Finance Manager			X	X		X

Example of a two person cash handling operation:

Roles	Receiving (handling) cash etc.	Preparing deposit	Reconciling receipts & deposits	Recording deposits to GL	Making cash deposits	Comparing deposits to GL entries
Individual 1 cash handler, custodian, alternate custodian	X	X			X	
Individual 2, Account supervisor, Reconciler, Dept Finance Manager			X	X		X

CHAPTER 6 - SECURING MULTNOMAH COUNTY BANK ACCOUNTS

Treasury has taken new measures to secure bank accounts due to increasing risk of bank account related fraud. Please instruct finance and related employees in your Department to implement this right away. Also, include this in your desk procedures and operational manual for current and new employee training.

Limit as much bank account information in your communication as possible.

1. DO NOT EMAIL BANK ACCOUNT NUMBER & BANK ROUTING NUMBER TO ANYONE IN THE COUNTY OR OUTSIDE
2. DO NOT ATTACH BANK STATEMENTS WITH FULL ACCOUNT NUMBERS IN YOUR EMAILS COMMUNICATIONS TO ANYONE IN THE COUNTY OR OUTSIDE
3. ALWAYS KEEP BANK ACCOUNT RELATED INFORMATION IN BANK STATEMENTS, BANKING SUPPLIES & FILES IN A SECURED LOCATION.
4. REQUEST TO OPEN / CLOSE BANK ACCOUNT, CHANGE BANK ACCOUNT INFORMATION, UPDATE SIGNATURE CARD, OPEN/CLOSE/CHANGE MERCHANT BANKCARD ACCOUNT WILL BE DONE THROUGH TREASURY ONLY
5. REQUESTS TO SIGN UP FOR ANY FORM OF ELECTRONIC PAYMENTS (ACH AND WIRE ENROLLMENT) SHOULD BE FORWARDED TO TREASURY FOR DECISION AND ACTION.

Please keep these in mind;
Know who you are communicating with. Check and confirm contact information whether in the county or outside (phone, fax, email address, bank location). USE ONLY LAST FOUR DIGITS OF THE BANK ACCOUNT NUMBER IN YOUR COMMUNICATIONS.

If you have to give full account number to bank for banking purposes you should call and positively identify the recipient of the information first. Get instructions as to how best and securely the information can be relayed. You might be asked to fax it to the number you get with attention to a specific person OR to send information via bank's secure email. Never give information on phone or otherwise unless you have established a positive ID.

If you have any question email treasury@multco.us and one of us will available to assist you.

'Historical practices shall not constitute justification for deviation from following policies and procedures set forth in the administrative procedures.'

CHPATER 7 – RESOURCES

FINANCE ADMINISTRATIVE PROCEDURES

https://commons.multco.us/administrative-procedures-and-executive-rules/multnomah-county-administrative-procedures

FIN-3: Obtaining Purchasing / Travel Cards and Other Lines of Credit
FIN-4: Miscellaneous Expense Reimbursements
FIN-5: Petty Cash Accounts & Cash Equivalents
FIN-6: Receipt and Deposit of County Funds
FIN-19: Accounts Receivable and Write Offs

MERCHANT RESOURCES

https://merch.bankofamerica.com/
https://www.pcisecuritystandards.org/
https://www.mastercard.us/en-us/merchants/get-support/security-training.html
https://usa.visa.com/visa-everywhere/security.html#2