

*<County Office Name>*

*U of MO Ext – County*

Credit Card Operations Guide

PCI DSS 3.2 Category 1&2

# Introduction

All Extension county offices that accept credit cards are required to have an operational guide for credit card transactions that details the steps required for handling credit card information, who is responsible for each policy, and how the policy is being enforced. An example of a completed guide can be found on the website for reference.

The ***U of MO Ext – County*** PCI DSS 3.2 credit card operations guide details the minimum requirements that ***U of MO Ext – County*** will adhere to for securing payments received and processed, whether on a dial-up terminal, cellular terminal, or by outsourced e-commerce website, as well as details who is responsible for each PCI DSS 3.2 policy and how that policy is being enforced.

# Terminal Usage

Only authorized individuals are allowed to process transactions on the terminal(s) and that authorization can only be granted by the ***County Program Director***. Documentation granting access to these individuals and a list of authorized users is on file with the ***Extension Statewide Fiscal Administration Team*.**

# Payment Processing

## Payments can only be processed in these approved ways:

## In-Person Payments

1. When a Customer comes into office to make payment, the staff member will enter all applicable information on the credit card payment form and the customer will sign the form to authorize payment to card. The staff member will verify the number, name on the card, expiration date, and amount to be charged on the credit card with the customer before processing the payment.
2. The staff member initials and dates the form, and either enters it into the Xon machine personally or gives it to the appropriate support staff for immediate entry into the Xon machine.
3. Payment is entered into Xon machine using information from the form.
4. Once payment is complete, the bottom of the form containing the credit card information is detached and cross-cut shredded and the Xon receipt is stapled to the top portion of the form.
5. If requested, a copy of the form and receipt is given to the customer
6. The original form is filed within a locked filing cabinet to which there is limited access and held for a period of no less than two years.

## Phone Payments

1. When a Customer calls the office and wishes to make a payment over the phone, the staff member will enter all applicable information on the credit card payment form for phone authorizations. The staff member will verify the number, name on the card, expiration date, and amount to be charged on the credit card with the customer before processing the payment.
2. The staff member initials and dates the form, and either enters the payment personally or gives it to the appropriate support staff for immediate entry into the Xon machine.
3. Payment is entered into the Xon machine using information from the form.
4. Once payment is complete, the bottom of the form containing the credit card information is detached and cross-cut shredded and the Xon receipt is stapled to the top portion of the form.
5. If requested, a copy of the form and receipt is mailed to the customer.
6. The original form is filed within a locked filing cabinet to which there is limited access and held for a period of no less than two years.

## Mail-in Payments

1. Customer mails in payment form with credit card information.
2. Staff member initials and dates the form, and either enters it into the Xon machine personally or gives it to the appropriate support staff for immediate entry into Xon machine.
3. Payment is entered into Xon machine using form.
4. Once payment is complete, the bottom of the form containing the credit card information is detached and shredded and the Xon receipt is stapled to the form.
5. If requested, a copy of the form and receipt is mailed to the customer.
6. The original form is filed within a locked filing cabinet to which there is limited access and held for a period of no less than two years.

## Fax Payments

1. When a Customer sends a payment via fax, a staff member will immediately remove the completed and signed form from the fax machine. That staff member will initial and date the form, and either enter the payment personally or give it to the appropriate support staff for immediate entry into either a Xon machine or QuickBooks.
2. Payment is entered into Xon machine or QuickBooks using information from the form.
3. Once payment is complete, the bottom of the form containing the credit card information is detached and cross-cut shredded and the Xon receipt is stapled to the top portion of the form.
4. If requested, a copy of the form and receipt is mailed to the customer.
5. The original form is filed within a locked filing cabinet to which there is limited access and held for a period of no less than two years.

# Payments can NEVER be accepted via email or RightFax fax-to-email. If a payment is received via one of these methods, the following procedure must be followed:

1. Write down the customer contact information
2. Delete the email and empty your trash can in Outlook
3. Contact the customer explaining that their email has been deleted and that you cannot accept their payment via email/fax. Let them know that you can accept payment by **phone, fax, mail, or in person**. Explain you are following policy to protect their personal information.
4. Follow your procedures for accepting payments above and process their payment using an approved acceptance channel.

# Network Transmission Policy

***All staff*** know and understand the policy that cardholder data is never to be sent via email or other non-secure end user messaging technologies.

# Refund Policy

Refunds should be submitted back to the same card that the original charge was processed. The ***County Support Staff*** are the only people authorized to issue refunds. ***County Support Staff*** will verify the last 4 digits of the card with the customer and then ask the customer for the full card number to process the refund back to the verified card. ***County Support Staff*** will hand key the card number and expiration date into the terminal and never write down the cardholder data on paper.

**Paper Storage/Destruction Policy**

Paper storage of card holder information for ***U OF MO EXT – COUNTY*** after authorization is not allowed under any circumstances. All cardholder data must be removed from the payment form and destroyed immediately after processing. In the event that transactions are not processed immediately, all paperwork containing cardholder data will be stored in a secure, locked location until processed. At no time should paperwork containing cardholder data be left unsecured unless it is being processed by staff. All paperwork containing cardholder data must be processed **within two business days after receipt**.

 **County Support Staff** is responsible for the destruction of cardholder data post-authorization. Cardholder data must be destroyed by the use of a cross-cut shredder.

# Vendor Supplied Defaults Policy

***County Program Director*** is responsible for the following or they know who is responsible and ***County Program Director*** will follow-up to ensure the requirements are being met:

1. Vendor-supplied defaults are always changed before installing a system on the network.
	1. Unnecessary default accounts are removed or disabled before installing a system on the network

# NOTE: vendor defaults could be accounts on a webserver that is hosted by the University and the webserver performs a URL redirect to the merchant gateway.

# Stored Cardholder Data Policy

***County Program Director*** is responsible for the following or they know who is responsible and ***County Program Director*** will follow-up to ensure the requirements are being met:

1. Sensitive authentication data is deleted or rendered unrecoverable upon completion of the authorization process
	1. Full contents of any track (from the magnetic stripe located on the back of the card, equivalent data contained on the ship, or elsewhere) are not stored after authorization.
	2. Card verification code or value (CVV) (three or four digit number printed on the front or back of a payment card) is NOT stored after authorization
	3. The personal identification number (PIN) or the encrypted PIN block is not stored after authorization
2. The PAN must be masked when displayed (the first six and last four digits are the maximum number of digits to be displayed) such that only staff with a legitimate business need can see more than the first six/last four digits of the PAN.

# User Authentication Policy

***County Program Director*** is responsible for the following or they know who is responsible and ***County Program Director*** will follow-up to ensure the requirements are being met:

1. User ID Policy
	1. All users are assigned a unique ID before allowing them to access system components or cardholder data.
	2. Access for any terminated users is immediately deactivated or removed.
2. In addition to assigning a unique ID, is one or more of the following methods is employed to authenticate all users:
	1. Something you know, such as a password or passphrase.
		1. User password parameters are configured to require passwords/passphrases to meet the following:
			1. A minimum password length of at least seven characters
			2. Contain both numeric and alphabetic characters
		2. Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.
	2. Something you have, such as a token device or smart card.
	3. Something you are, such as a biometric.
3. Group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows:
	1. Generic user IDs and accounts are disabled or removed;
	2. Shared user IDs for system administration activities and other critical functions do not exist; and
	3. Shared and generic user IDs are not used to administer any system components

**NOTE: The systems that the User Authentication Policy refers to could be a University hosted web server that performs a URL redirect to the merchant gateway. The User Authentication Policy could also be applied to the accounts used to access the merchant gateway, event mgmt. system, donor mgmt. system, continuing education system, etc.**

# Security Policy

All employees that come into contact with customer cardholder data within the county offices using the ***U OF MO EXT – COUNTY*** merchant are responsible for protecting cardholder data.

The ***County Program Director*** is responsible for establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations. All authorized usersare responsible for reporting any suspected data breaches to the **County Program Director.** The ***County Program Director*** is responsible for gathering all relevant information and reporting any suspected data breaches to the ***Extension PCI contact***, who will forward the information to the appropriate campus contact. The ***County Program Director*** is responsible for meeting with the ***Extension PCI contact*** and campus information security officer not more than one week following the incident to review the results of the investigation to determine the root cause of the compromise and evaluate the effectiveness of the incident response plan.

# Security Training

The ***County Program Director*** is responsible for the formal security awareness program to make all personnel aware of the cardholder data security policy and procedures, as well as security training for all new hires and existing staff**.**

The ***County Program Director*** will use the [new hires checklist](http://umurl.us/2qC) to perform the following:

1. Have all relevant staff read, understand, and attest that they have read and understood the merchant specific policies and procedures.
2. Have all relevant staff read, understand, and attest that they have read and understand the University credit card policy (<http://umurl.us/7Fk>)
3. Have the new hire complete the cardholder data processing agreement & annual training form (<http://umurl.us/lo5hO>)
4. Contact the ***Extension PCI contact*** to have your new hire enrolled into the appropriate online training upon hire. New hires are enrolled at the beginning of each month.
	1. New hires must complete the online training upon hire and annually thereafter.
5. Train the new hire with specific functional training as it relates to their job duties.
	1. For example, train them to use the specific terminal or point of sale device that they will be processing transactions on. This training should include the desk manual that you develop.

# Terminal Physical Security

The ***Extension PCI contact*** for ***U of MO Ext - County*** is responsible for developing and maintaining a [Capture Device Inventory Log](http://umurl.us/TBNbD). The ***Extension PCI contact*** for ***U of MO Ext - County*** is responsible for making sure the inventory log has the following minimum requirements:

1. Make/Model of the terminal(s)
2. Location of the Terminal(s)
3. Serial number or unique identification number of the terminal(s)
4. Serial number(s) of the tamper tape that was added to the swipe devices.

***County Program Director*** is also responsible for maintaining the log so that it is updated anytime a new device is added, relocated, no longer in use, etc. and notifying the ***Extension PCI contact*** of those changes. If any device the merchant has is a cellular device and is mobile then a [Cellular Terminal Log](http://umurl.us/CHh7X) must be maintained by ***County Program Director*** detailing where the device is and who is in possession of it at all times.

***County Program Director/assigned staff*** is responsible for inspecting all terminals to look for tampering or substitution using the [Capture device Periodic Inspection Form](http://umurl.us/nvP9) every 3 months or if the terminals are open to the public then once every month. Those forms are required to be emailed to the ***Extension PCI contact*** upon completion.

***County Program Director*** is responsible for training ***ALL staff*** to be aware of attempted tampering or replacement of devices as follows:

1. **ALL** staffmustverify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
	1. Only Commerce Bank is authorized to access, modify, or trouble shot devices.
	2. ***County Program Director/assigned staff***will call Commerce Bank at 800-828-1629 to initiate the access.
2. Nostaff memberwillinstall, replace, or return devices without verification by ***County Program Director***.
3. All staffwill be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
4. All staff will report suspicious behavior and indications of tampering or substitution to ***County Program Director*** immediately.

The terminal physical security policies and operational procedures is documented, in use, and known to all affected parties.

# Incident Response Policy

In the event of security incident or breach, employees are required to take steps to preserve any evidence of the incident and report the incident **IMMEDIATELY** to their ***County Program Director***, who will then contact the Extension PCI contact to report the incident and obtain further guidance. The Extension PCI contact will relay information regarding the breach to the Information Security Officer for the university and will serve as a liaison in all further proceedings involving a breach. Employees should not communicate with anyone about the incident outside of their supervisor(s), the Extension PCI contact, or the Information Security Officer.  Document all known facts while waiting for the Information Security Officer to respond, including date, time, and the nature of the incident.  This will aid in responding in a more appropriate manner.

**If the incident involves a compromised computer system, do not alter the state of the computer system. The following must be done:**

* **Do not shutdown the computer or restart the computer.**
* **Immediately disconnect the computer from the network by removing the network cable from the back of the computer.**
* **The computer system should remain on and all currently running computer programs left as is.**

# Service Providers Policy

*(If you need help contacting or knowing the correct questions to ask your 3rd party please contact* *pci@missouri.edu**)*

***Extension PCI contact*** is responsible for the following as it pertains to managing third party service providers:

1. Maintain a list of all service providers that ***U of MO Ext - County*** uses to maintain their cardholder data environment and that list must also include a description of the services provided by each service provider.

|  |  |
| --- | --- |
| **Service Provider Name** | **Service(s) Performed** |
| First Data Merchant Services | Payment processor |
| Commerce Bank | Acquiring bank |

1. Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (or otherwise process, transmit, or store) on behalf of ***U of MO Ext - County*** or to the extent the 3rd party could impact the security of ***U of MO Ext – County*** cardholder data environment
2. ***U of MO Ext – County*** will complete the [3rd party checklist](http://umurl.us/BYBq8) whenever a new 3rd party service provider is to be added to the cardholder data environment to ensure proper due diligence.
3. Monitor all service provider’s PCI DSS compliance status at least annually
4. Maintain information about which PCI DSS requirements are managed by each service provider, and which requirements are managed by ***U of MO Ext - County*.**

This office, operating under the ***U of MO Ext – County*** merchant,has read and understands the Merchant Operational Policies and Procedures above and agrees to follow the Merchant Operational Policies and Procedures.This document is required to be kept on file within the unit and a signed copy supplied to the Extension fiscal administration team. If revisions are made, the unit is responsible for supplying an updated copy to the Extension fiscal administration team.

By the signature below, this information is a true and factual representation of our business processes.

**Office Name** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**CPD Signature** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Date** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Information Security Responsibilities**

It is the responsibility of every staff member to protect cardholder data and university assets designated to process such data. University of Missouri Extension has provided a credit card policy to augment your unit’s specific policies and procedures in an effort to strengthen all necessary controls over the credit card processing environment.

By your signature below, you attest that you have read and understand the Credit Card Operations Guide specific to your unit and the Extension Credit Card Policy and agree to follow all applicable operational policies and procedures regarding the protection of cardholder data and unit assets for processing that data. Furthermore, you understand that violation of these policies and procedures may result in disciplinary action up to, and including, possible termination from my position.

**Employee Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_**

**Supervisor Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_**