

Credit Card Policy

Revised 12/14

# Personnel Training

The [University’s credit card policy](http://umurl.us/7Fk) states, *“Any official, administrator, or affiliate with responsibilities for managing University cardholder transactions and employees or personnel entrusted with handling or processing cardholder payments must complete annual training.” Please see the* [*Cardholder Data Processing Agreement and Annual Training Form*](http://umurl.us/lo5hO) *for more information.* All new hires that will have credit card handling duties and those with new duties that require credit card processing must also complete an [Extension Credit Card Processing Checklist](#_Extension_Credit_Card) which includes training requirements for both initial and annual training.A copy of the checklist can be found in Appendix A.

The checklist includes the following steps-

* All new hires must be given a copy of the merchant policies and procedures pertaining to the unit in which they will be working, as well as a copy of the [University Credit Card Policy](http://umurl.us/7Fk).
* All employees must have a completed [Cardholder Data Processing Agreement & Annual Training Form](#_Cardholder_Data_Processing) on file with their operational unit. A copy of this form must also be emailed to AMT Fiscal so that employees may be enrolled in training. This form is required to be presented on request by the unit.
	+ New hires are enrolled at the beginning of each month.
	+ Regular staff will get training through [SANS](https://sso.securingthehuman.org/umsystem)
	+ County office staff and student workers will get training through Extension’s [Blackboard system](https://bblearn.missouri.edu/webapps/portal/frameset.jsp).
* New hires are given unit-specific training on all applicable equipment and unit processes.

Additionally, all employees who handle credit card data must complete annual training offered by the Treasurer’s Office. The Treasurer’s office will notify individuals of required annual training opportunities, but annual training compliance is the responsibility of the department, continuing education unit, or county office to which the employee is assigned.

# Definitions

* **Cardholder Data** – 16-digit PAN (primary account number), cardholder name, and expiration date
* **Sensitive Authentication Data (SAD)** – Magnetic stripe data or chip equivalent, security code (CVV/CVC/CVV2/CVC2), and personal identification number (PIN)
* **Card Verification Value (CVV/CVC)** – unique security code on the back of the credit card that aids in authenticating card information
* **Merchant** - A merchant is a department, entity, or affiliate that accepts cardholder payments using the university’s merchant processor(s). A University merchant is assigned a merchant account number by the Office of the Treasurer.
* **Electronic Credit Card (ECC)** - A PeopleSoft application that takes the end of day files from the card processor (First Data Merchant Services) and posts it to the general ledger (GL).

# Processing, Storing, and Transmitting Data

## **Data Retenti**on

The records retention policy for the University requires credit card receipts to be retained for no less than 2 years. This is important because the transaction record required by the policy may be the same record needed to defend a customer dispute or chargeback at a later date. All documents containing credit card information must be kept in a locked drawer or filing cabinet and accessible only by authorized personnel. Credit card payment information should never be left unattended on a desk, computer screen, or in a public area.

## Receiving Payments via Email and Other Messaging Technologies

Cardholder data MAY NOT be, under any circumstances, emailed, scanned, or sent via instant messaging. If a customer sends cardholder data via an unapproved method, they must be notified that the transaction cannot be processed and the email deleted. If a customer e-mails or sends cardholder data via an unapproved method, Extension staff must take the following steps:

1. Notify customer that the transaction cannot be processed
2. Request that cardholder data be provided via telephone
3. Delete the email completely using the Shift + Delete keys; if received via a non-approved fax machine, the entire form should be cross-shredded.

## Receiving Payments by Fax

Credit card information received via fax must only be done through a standard phone line connected fax machine. With recent updates to University fax/copier systems it is recommended that credit card information not be transmitted via fax, unless you can document which fax machine you are using and that it is connected through a standard, dedicated phone line. University offices must contact the Office of the Treasurer to have your fax machine and connection audited before you can accept fax credit card payments. County program directors will be responsible for providing documentation that validates the line to which the fax machine is connected is a dedicated phone line for county offices. After a faxed payment has been processed, the document must be handled in the same way as any other credit card payment documentation.

## Shredding and Destroying Cardholder Data

Cardholder data must be destroyed when it is no longer needed for business or legal reasons. Paper documents must be **cross-cut shredded**. If a service provider vendor is used to destroy cardholder data, the vendor must be a Level 1 service provider on the approved PCI list or be approved by NAID, National Association Information Destruction. Please contact Extension fiscal administration for approved vendors.

## Credit Card Numbers

All forms designed to capture credit card information **MUST** be designed to have the card number at the bottom of the form. After the card number is processed, the portion of the form with the card number should either be cut off and destroyed in a cross-cut shredder or, if the form is kept, it must be securely stored per the instructions below. Forms containing the unmasked sixteen digit card numbers must **NOT** be scanned for any reason.

## CVV2 validation code or PIN number

Under no circumstances should office staff be in possession or have knowledge of a customer’s CVV/CVC (three or four digit validation code on back of card) or PIN (personal identification number). This information should not be recorded on any form or other medium for any reason.

## Masking of Card Numbers

Terminals, computers, and receipts may display or print no more than the last four digits of the credit card number; the rest of the card number must be obscured from view. On forms requiring the full 16-digit credit card number, the first twelve digits must be redacted on the form after processing the payment by using a marker or other medium to completely obscure the number. The blacked-out form then must be copied and the original form destroyed. The copied form would then be included with other transaction documentation.

# Procedures

Credit card payments that have been mailed to the unit should be routed for immediate entry by office staff. If they will not be entered immediately, forms must be stored securely in a locked drawer or cabinet until such time as they can be entered. All documents containing credit card information must be kept in a locked drawer or filing cabinet and accessible only by authorized personnel. Credit card payment information should never be left unattended on a desk, computer screen, or in a public area.

## Payment Procedure

* Information is received either via phone, in person, or faxed form; for phone and in-person transactions, office staff will complete the credit card payment form.
* Form is routed for immediate entry. Credit card information should be keyed immediately into XON, but if it is not entered immediately, form should be stored securely until the information can be entered.

## Receipts

All credit card payment transactions require a receipt be provided to credit card holder. The receipt must include:

* Payment type
* Customer Name
* Purpose of payment
* Amount paid for each item
* Payment date
* Name of person issuing receipt

The receipt form can be emailed, faxed, scanned, or provided in person to the cardholder. The merchant must retain a copy of the receipt for bookkeeping purposes, but it may not contain any credit card information other than name and amount. The customer/cardholder must be given a copy and a copy must be retained by the merchant location for not less than two (2) years.

For those offices without a standard form for recording information in credit card transactions, a template will be provided on the website.

## Refunds

When a customer requests a refund, the staff member must verify the cardholder’s information. They will need to provide the entire credit card number to the office staff for a refund to be processed. Documentation for credit card refunds should be handled in the same way as payment receipts.

# Enforcement

Everyone in Extension has a duty to protect our customers’ credit card information. It will be the responsibility of each unit’s director to ensure that all applicable PCI data security standards are adhered to within their unit. Responsibility for adherence to these standards within the county extension offices are the responsibility of each county program director with oversight from the regional director. All units and county offices utilizing University-provided ecommerce or other credit card processing solutions are subject to compliance audits by members of the University of Missouri Extension’s statewide fiscal administration team or regional staff. In the event that an office is found to be out of compliance with this policy, the office may face additional fees for non-compliance and repeated violations could result in loss of the office’s capability to process credit cards through the University.

# Extension Credit Card Processing Checklist

Training upon hire and annually

The credit card policy states, *“Any official, administrator, or affiliate with responsibilities for managing University cardholder transactions and employees or personnel entrusted with handling or processing cardholder payments must complete annual training. Please see the “Cardholder Data Processing Agreement and Annual Training Form”.*

* Give the new hire a copy of your unit’s policies and procedures and a copy of the [Extension Credit Card Policy](http://extension.missouri.edu/staff/fiscal/documents/MU%20Extension%20Credit%20Card%20Policy.docx) for their review and for them to keep as their own.
* Have the new hire complete the [Cardholder Data Processing Agreement & Annual Training Form](http://umurl.us/lo5hO).
	+ This form should be retained in the office for documentation and is to be presented upon request.
	+ Forward a copy of the form to AMT Fiscal (muextamtfiscal@missouri.edu) to have your new hire enrolled into the appropriate online training upon hire. New hires are enrolled at the beginning of each month.
	+ New hires must complete the online training upon hire and annually thereafter.
		- Regular University staff go through [SANS](https://sso.securingthehuman.org/umsystem)
		- Students and county office staff go through [MU’s Blackboard](https://bblearn.missouri.edu/webapps/portal/frameset.jsp)
* Train the new hire with specific functional training as it relates to their job duties.
	+ For example, train them to use the specific terminal or point of sale device that they will be processing transactions on.

# Cardholder Data Processing Agreement and Annual Training Form

*Revised 08/25/2014*

**Why Should I Know the University Credit Card Policy?**

It is important to protect customers’ credit and debit card numbers for many reasons:

* To protect the University’s customers from fraud.
* To protect the University from onerous fines and penalties levied by the credit and debit card companies in the event of a credit card breach.
* The University will take appropriate corrective action up to and including termination and/or criminal action against employees who violate the University Credit Card policy.

As a credit card processor I agree to abide by the provisions in this document and the University “Credit Card Policy.”

**What Should I Know?**

**Cardholder data** – refers to displaying or printing more than the last four digits of a customer’s sixteen (16) digit number credit or debit card number. It also includes “Sensitive Authentication Data” which refers to the three (3) or four (4) digit CVV2 validation code on the front or back of a card or the PIN number, personal identification number. PCI does not permit Sensitive Authentication Data to be stored even if protected according to the PCI Data Security Standards.

The following are things you should **NEVER** do:

* + **NEVER** acquire or disclose any cardholder data without the cardholder’s consent.
	+ **NEVER** store or write down on paper or in electronic form the three (3) or four (4) digit security code (CVV2, CID, CAV2) from the front or back of a card or a PIN, (personal identification number).
	+ **NEVER** transmit, send or receive cardholder data by e-mail, Right Fax, Image Now or other end-user messaging technologies.
	+ **NEVER** scan any form that includes cardholder data.
	+ **NEVER** share a computer password that has access to a computer with cardholder data.
	+ **NEVER** leave sensitive information on your desk, screen, or in any public area.

I **WILL DO** the following:

* + At time of employment, agree to complete a background check within the limits of local law.
	+ At time of employment and annually, agree to complete annual PCI and security training. <http://www.umsystem.edu/ums/fa/treasurer/training>
	+ Escort and supervise all visitors including University personnel in areas where cardholder data is maintained.
	+ Store all physical documents or storage media containing cardholder data in a locked drawer, locked file cabinet, or locked office with a business need to know access.
	+ Destroy cardholder data using a cross-cut shredder or with an approved service provider.
	+ Report immediately a credit or debit card security incident to my supervisor and the appropriate Information Security Officer if I know or suspect card information has been exposed, stolen, or misused.
		- <http://infosec.missouri.edu/admin/iso.html>

(This report **must** **not** disclose by fax or e-mail cardholder data, three or four digit validation codes, or PINs.)

* + Place your terminal in a secure location and regularly inspect the terminal for skimming devices.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Employee Signature Employee Printed Name Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Supervisor Signature Supervisor Printed Name Date

**<Insert Logo Here>**

< Street Address>

< City State Zip>

< Phone Number>

**Credit Card Payment/Refund Authorization Form**

Sign and complete this form to authorize <insert business name> to make a one-time debit/credit to your credit card listed below.

By signing this form you give us permission to debit/credit your account for the amount indicated. This is permission for a single transaction only, and does not provide authorization for any additional unrelated debits or credits to your account.

**Please complete the information below:**

I \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ authorize <Insert Business Name> to charge my credit card

 (full name)

account indicated below for \_\_\_\_\_\_\_\_\_\_\_\_\_ on or after \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. This payment is for

 (amount) (date)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (description of goods/services)

Billing Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Phone# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

City, State, Zip \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Email \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SIGNATURE ­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ DATE**

**I authorize the above named business to charge the credit card indicated in this authorization form according to the terms outlined above. This payment authorization is for the goods/services described above, for the amount indicated above only, and is valid for one time use only. I certify that I am an authorized user of this credit card and that I will not dispute the payment with my credit card company; so long as the transaction corresponds to the terms indicated in this form.**

|  |
| --- |
| Account Type: [ ]  Visa [ ]  MasterCard [ ]  AMEX [ ]  Discover Cardholder Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Account Number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Expiration Date \_\_\_\_\_\_\_\_\_\_\_\_  |

**<Insert Logo Here>**

< Street Address>

< City State Zip>

< Phone Number>

**Credit Card Payment/Refund Phone Authorization Form**

Sign and complete this form to authorize <insert business name> to make a one-time debit/credit to your credit card listed below.

By signing this form you give us permission to debit/credit your account for the amount indicated. This is permission for a single transaction only, and does not provide authorization for any additional unrelated debits or credits to your account.

**Please complete the information below:**

I \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ authorize <Insert Business Name> to charge my credit card

 (full name)

account indicated below for \_\_\_\_\_\_\_\_\_\_\_\_\_ on or after \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. This payment is for

 (amount) (date)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

 (description of goods/services)

Billing Address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Phone# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

City, State, Zip \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Email \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SIGNATURE ­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­­\_\_Per Phone Authorization\_ DATE**

**I authorize the above named business to charge the credit card indicated in this authorization form according to the terms outlined above. This payment authorization is for the goods/services described above, for the amount indicated above only, and is valid for one time use only. I certify that I am an authorized user of this credit card and that I will not dispute the payment with my credit card company; so long as the transaction corresponds to the terms indicated in this form.**

|  |
| --- |
| Account Type: [ ]  Visa [ ]  MasterCard [ ]  AMEX [ ]  Discover Cardholder Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Account Number \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Expiration Date \_\_\_\_\_\_\_\_\_\_\_\_  |