**Credit Card Loaner Machine Policy**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Policy Statement**

**------------------------------------------------------------------------------------------------------------------------------------------**

**Who should know this policy?**

Any official or administrator with responsibilities for managing University credit card transactions and those employees entrusted with handling or processing credit card information. This includes fiscal officers and system managers.

**To whom this policy applies**

This policy applies to all units and or departments that wish to use a credit card loaner machine from the Office of the Treasurer.

**Policy revision history**

|  |  |  |
| --- | --- | --- |
| Initial Publication | John Layman | 01/2013 |
| Annual review | John Layman | 01/2014 |
| Annual review | John Layman | 01/2015 |
| Annual review | John Layman | 01/2016 |
| Annual review and update | John Layman | 01/2017 |
| Annual review | John Layman | 01/2018 |
| Annual review | John Layman | 01/2019 |
| Annual review | John Layman | 01/2020 |
| Annual review | John Layman | 01/2021 |
| Annual review | John Layman | 01/2022 |
| Annual review and update | John Layman | 04/2023 |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**General Responsibilities and Requirements**

------------------------------------------------------------------------------------------------------------------------------------------

**Responsibilities of the Office of the Treasurer**

* Communicate the policy and PCI DSS to those the machine is loaned to.
* Distribute a quick reference guide for the credit card machine to those the machine is loaned to.
* Update the Electronic Credit Card PeopleSoft Application (ECC). This is a PeopleSoft application that takes the end of day file from the card processor (JPMorgan Chase Paymentech) and posts it to the general ledger (GL).
* Obtain signatures from those who will be processing credit card payments attesting they understand the policies and procedures and will follow the policies and procedures.
* Visually inspect the terminal for any tampering or skimming before and after the terminal is loaned out.
* Update the capture device log to maintain the make/model of the device loaned out, location of the device, serial number of the device, who has checked out the device, and when it is going to be returned.
* Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.
* Communicate the security awareness program to those checking out the terminal.
* Manage all 3rd party service providers who support the loaner machine merchant environment.
* Review the policy at least annually.

**Responsibilities of those receiving the loaner machine**

* All those who will be processing credit card payment must read and understand the credit card loaner machine policy.
* All those who will be processing credit card payments must sign the attestation form attached and present it to the Office of the Treasurer.
* All those who will be processing credit card payments must know to be aware of the following:
  + Verify the identity of any third party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices
  + Do not install, replace, or return devices without verification
  + Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices)
  + Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer)
* Always construct your mail order forms so that the contact and registration information is at the top and the payment information is at the bottom of the form.  This allows you to tear off the payment information portion to destroy by cross cut shredder and allows you to retain the top portion for your records. The card holder data must be destroyed post authorization.
* Always return the machine and all accessories back to the Office of the Treasurer.
* Never write down or store the CVV code post authorization.
* Never send the credit card number (PAN) by unsecure end user messaging (email).

If processing in person payments:

* Machine must only be using dial up connection through an analog phone or fax line.
* Only those that have signed the last page of this policy document are allowed to process or handle credit card payments.
* Never write down card information for processing later (Credit Card Number, CVV, etc.).
* Have customer sign the merchant receipt copy and retain for your records.  Always offer the customer receipt copy for their records.
* Batch the machine each day to settle the day’s transactions.
* Keep the machine in a secured location.
* Never leave the machine unattended.
* Paper storage should consist of only credit card receipts or batch settlements statements and those can only include the last 4 of the customer card number.
* Report any suspected or known security threat or incident per the [Incident Response Policy](https://www.umsystem.edu/ums/is/infosec/hr-mandatory-reporting).

If processing mail order payments:

* Machine must only be using dial up connection through an analog phone or fax line.
* Never request CVV2.  It is not needed for mail order transactions and is not permitted to be stored electronically nor on paper.
* Construct your mail order forms so that the contact and registration information is at the top and the payment information is at the bottom of the form.  This allows you to tear off the payment information portion to destroy by cross cut shredder and allows you to retain the top portion for your records. The card holder data must be destroyed post authorization.
* Keep merchant receipt copy and retain for your records.  Always offer the customer receipt copy for their records.
* Batch the machine each day to settle the day’s transactions.
* Keep the machine in a secured location.
* Never leave the machine unattended.
* Paper storage should consist of only credit card receipts or batch settlements statements and those can only include the last 4 of the customer card number.
* Report any suspected or known security threat or incident per the [Incident Response Policy.](https://www.umsystem.edu/ums/is/infosec/hr-mandatory-reporting)
* Link to a quick reference guide
  + [Dial up Vx520 terminal](https://merchantservices.chase.com/content/dam/chase/merchant-services/support/us/documents/quick_reference_guide_verifone_vx.pdf)
  + [Cellular Ingenico MOVE 5000 4G terminal](https://merchantservices.chase.com/content/dam/chase/merchant-services/documents/desk-move-5000-reference-guide.pdf)

Please describe your event you are obtaining the Treasurer’s loaner machine for

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

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

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

MO code / PS account for revenue\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

MO code for transaction fees\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date you will pick up the terminal\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date you will return the terminal\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**As a credit card handler or processor I agree to abide by the provisions in this document. Please sign and present this portion to the Office of the Treasurer (*Please keep a copy for your files).***

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

**Signature** **Date**

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

**Print Name Email**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**University Department**

***Please sign the next page as well. Please scan and email or bring both signed forms to the Office of the Treasurer when you pick up your loaner terminal.***

**Loaner Terminal Processing Agreement and Training Form**

*Revised 04/2023*

**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:

* Construct all forms so that the cardholder information is located at the bottom of the form. After authorization the bottom portion of the form is removed that contains cardholder data and destroyed by cross cut shredder or all but the last 4 of the credit card number (PAN) is removed by a hole punch.
  + Escort and supervise all visitors including University personnel in areas where the loaner terminal is maintained while you have it in your possession.
  + Paper storage will consist of only credit card receipts or batch settlements statements and those can only include the last 4 of the customer card number.
  + Report immediately a credit or debit card security incident to your supervisor and the appropriate [Information Security Officer](https://www.umsystem.edu/ums/is/infosec/iso) if you know or suspect card information has been exposed, stolen, or misused.

(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 and or substitution.

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

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

Supervisor Signature Supervisor Printed Name Date