**Annual Policy Acknowledgement Form**

*Revised 02/22/2017*

**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 merchant, I agree to read, understand, and follow the provisions in this document, my merchant specific policies and procedures, and the University “[Credit Card Policy](http://umurl.us/7Fk).”

**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.
    - <https://www.umsystem.edu/ums/is/infosec/iso>

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

* + Keep a log of all of my swipe devices using the [capture device inventory log](http://umurl.us/TBNbD).
  + Keep a log of my physical inspections using the [capture device periodic inspection log](http://umurl.us/FI4).
  + Place your terminal in a secure location and periodically inspect the terminal for tampering and substitution using the [capture device periodic inspection procedures](http://umurl.us/nvP9).

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

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

Supervisor Signature Supervisor Printed Name Date