CREDIT CARD PROCESSING GUIDELINES

After a review of the credit card pre-assessment questionnaires that each department completed, there are a number of items that warrant additional guidance in regards to appropriate storage/processing/transmission of credit card data.

Our main areas of concern are:

1. Storage of cardholder data
2. Receiving/Sending cardholder data via email or instant messaging
3. Virtual Terminals/Entering card information online for customers/registrants
4. Credit card information received via FAX

While most departments are adhering to the below guidelines, it is important that we remind everyone about these regulations as it could impact your ability to accept credit card payments in the future. As part of the overall assessment process these items will be reviewed. If it is found that as a merchant you are not adhering to these items it would require immediate remediation, or cancellation of your merchant account. For any additional questions please refer to the University of Missouri credit card policy located at the link below.

http://www.umsystem.edu/ums/fa/treasurer/payment_card_policies

1. Storage of Cardholder data

PCI DSS Requirement 3.1

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements
- Processes for secure deletion of data when no longer needed
- Specific retention requirements for cardholder data
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention

Paper storage of the full credit card number is allowed if a formal data retention policy is in place for each merchant. The policy should outline the controls maintained over the data and indicate where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. It is recommended that University merchants **DO NOT** store the full credit card number unless there is a specific business need.

The only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. **Storing this information in an Excel file is NOT ALLOWED!** If you are storing the full card number in an Excel file it must be truncated or deleted immediately. Storage of the security code is never allowed.

PCI DSS Requirement 3.4

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography, (hash must be of the entire PAN)

- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

Storage, either electronically or on paper, of the card verification code or value (CVV) is **never** allowed.

> PCI DSS Requirement 3.2.2
> **3.2.2** The card verification code or value (three-digit or four-digit number printed on the front or back of the payment card) is not stored under any circumstance.

If you need guidance on how to properly remediate your paper storage please contact the Treasurer's Office as soon as possible. If you are using the CVV to validate the card transaction, it is suggested to ask for the billing zip code as verification method.

If you are collecting credit card data on a form, it is recommended to construct the form with the credit card information section at the bottom. After the payment has been processed, the credit card information can be removed from the form and cross cut shredded. Lastly you can attach the receipt to the top portion of the form (that contains no card holder information) and retain for your records.

2. Receiving/Sending credit card information via email is NOT ALLOWED!

> PCI DSS Requirement 4.2
> **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

E-mail, instant messaging, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. **DO NOT** utilize these messaging tools to send or receive credit card information. **This includes email attachments with credit card information or fax emails.** If someone sends credit card information through email, the information must be deleted and you must notify the person that we are unable to process credit card data received via email.

3. Virtual Terminals – Web application or entering credit card information on behalf of a customer

A virtual payment terminal is web-browser based access to an acquirer, processor, or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser.

Using a virtual terminal, entering credit card information on behalf of a customer, or directing someone to a University owned computer to enter credit card information requires specific controls around that computer. The computer must be in a single, isolated, location, and not connected to other locations or systems within your environment. Isolation of the system can be achieved via firewall or network segmentation. You **CAN NOT** use your normal desktop workstation as a virtual terminal as it is connected to other systems and environments.

Any department using a virtual terminal or entering card information on behalf of the customer **must** review and choose one of the following solutions to remain in compliance.

- Setup an isolated computer/workstation to PCI DSS standards for the sole purpose of processing credit card information. This workstation must not be connected to any other computer/system within your environment or used for email, etc.
- Review/change business policy and procedures to no longer allow staff to process credit card information through their web based application on behalf of a customer.
- Discontinue use of the virtual terminal, and process credit card transactions through a standard dial up or IP connected credit card machine.

4. Receiving/Sending card information via 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. Adoption changes to business policies and procedures to no longer accept credit card information via fax is recommended for all merchants if possible.

I understand that these items require additional changes to procedures that have been in place for some time, but it is imperative that these changes are made immediately as our deadline for PCI compliance is quickly approaching. If you are unable to make these necessary changes or need additional guidance, please let us know as soon as you can.