**POLICY**

Issued: 02/07/2014

Revised: 08/16/2015

Revised: 02/22/2017

Revised: 11/14/2018

Revised: 03/03/2023

Revised: 06/26/2024

The University’s Merchant Policy requires all merchants and personnel accepting and processing credit and debit cards to comply with the current version of the Payment Card Industry’s (PCI) Data Security Standards (DSS). <https://www.pcisecuritystandards.org/document_library/>

University merchants using third party service providers to process cardholder data must use Level 1 service providers or service providers who have been audited and submitted an AoC, (Attestation of Compliance) or SAQ Service Provider. When establishing a relationship with a new service provider the University must complete the [3rd Party Service Provider Checklist](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/3rd_Party_Checklist.docx?d=w1f1f7e4b799e4d28a56643a2c720dfb8) prior to engagement. Service providers must maintain PCI compliance and the department must monitor the annual renewal date of compliance.

**Definitions (also see definitions at the end of this document)**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Cardholder Data** | 16-digit PAN (primary account number)Cardholder nameExpiration date |
| **Sensitive Authentication Data** | Magnetic stripe data or equivalent on a chip Security code – CVV, CVC2, CVV2PIN (personal identification number for debit cards)  |
| **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.  |

**Policy Details**

**Who Should Know This Policy**

Any official, administrator, or affiliate with responsibilities for managing University cardholder transactions and employees or personnel entrusted with handling or processing cardholder payments.

This policy applies to merchants which store, process, or transmit cardholder data. This includes merchants which accept credit card payments using terminals, any manual (paper) process, point-of-sale transactions, and internet (e-commerce) transactions. Internet transactions include links on University websites or 3rd party hosted websites redirecting customers to another website or gateway for payment. The University Merchant Policy requires each department that accepts cardholder payments be approved by the Office of the Treasurer and, where applicable, validated by the University’s external PCI assessor.

**Background Information**

The cardholder industry formed a council called the Payment Card Industry Council which includes Visa, MasterCard, American Express, and Discover. This PCI Council has developed Data Security Standards (DSS) to assure consumers that using credit and debit cards are secure. These standards include controls for handling credit and debit cards, computer and Internet security, and reporting of a breach of cardholder data. These standards are mandated by the industry in order for a merchant to accept cardholder payments.

Although the primary focus of PCI DSS is on Internet-based transactions, there are other services that allow systems to be Internet accessible which may expose cardholder information. Basic functions such as e-mail can result in Internet accessibility of a merchant’s network. Therefore, all University merchants, including merchants transmitting via a stand-alone terminal, must complete an annual audit, and, if applicable, an internal scan and a remote external scan by our PCI approved vendor.

In the event of a breach of cardholder data at a merchant location, our University merchant processor is authorized on behalf of the cardholder companies to assess the merchant any fine levied by the card associations as well as the costs of investigation, remediation, customer notification, and customers’ card re-issuance.

**PROCEDURE**

Issued: 02/07/2014

Revised: 08/16/2015

Revised: 02/22/2017

Revised: 11/14/2018

Revised: 03/03/2023

Revised: 06/26/2024

**Processing Methods and Applicable Data Security Standards**

The University has identified 9 categories of merchants based on how they process cardholder data. Please note, these are general guidelines; the University, with assistance of an external PCI assessor may require additional PCI requirements be met. For full details on merchant categories see below:

**Category 1** – All credit card processing is outsourced

**Category 2** – Merchant only processes payments using a dial up (copper phone Line or cellular) terminal.

**Category 3** – Transmit and process cardholder data via payment applications but cardholder data is not stored

 electronically.

**Category 4** – Merchant only processes payments using a web-based (virtual terminal), and does not store

 cardholder data electronically.

**Category 5** – Merchant only processes payments with a payment application system connected to the internet with NO electronic cardholder data storage.

**Category 6** – Merchant which stores cardholder data in electronic format, or do not fit in categories 1 through 5.

**Category P2PE** – Merchant who only process payments using hardware payment terminals included in a validated and PCI SSC-listed PCI point-to-point encryption (P2PE) solution.

**Category SAQ A-EP** – Merchants who have a partially outsourced E-commerce website using a third-party website for the payment processing.

**Category SAQ SPoC** – Merchants using a commercial off the shelf mobile device (for example phone or tablet) with a secure card reader that is a part of a SPoC Solution included on the PCI SSC’s list of validated Software-based PIN Entry on COTS (SPoC) Solution.

**E-commerce Processing**

The preferred method for accepting e-commerce payments is for customers to be redirected to a PCI approved third party service provider to transmit, process, and/or store cardholder data.

**PCI Policies and Procedures**

All merchants must adopt and maintain [PCI-specific policies and procedures](https://www.umsystem.edu/ums/fa/treasurer/payment_card_policies) commensurate with their merchant category. The University will provide policy and procedure templates. Merchants will be responsible for revising templates as needed to correspond with payment environments. In addition, merchants will be responsible for ensuring their policies and procedures are periodically reviewed, and that all staff understands the policies and procedures, and understand their roles in maintaining compliance.

**Third Party Service Providers**

When establishing a relationship with a new service provider the University must complete the [3rd Party Service Provider Checklist](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/3rd_Party_Checklist.docx?d=w1f1f7e4b799e4d28a56643a2c720dfb8) prior to engagement. Service providers must maintain PCI compliance and the department must monitor the annual renewal date of compliance.

**Establishing or Making Changes to a Merchant Account**

In order to accept credit or debit cards a department must complete a “[Cardholder Merchant Agreement and Request Form”](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Merchant_Request_Form.docx?d=w27f4e88c0e8e4029b6b9b75734b13ade) and return it to the Office of the Treasurer. If the merchant is using a third-party service provider, this provider must sign a service provider contract. Changes to an existing merchant account must be submitted to the Office of the Treasurer. In addition, prior to making changes to merchant category or processing method, the merchant must provide a compliance plan. Examples of changes are: purchasing, selling, or discarding a terminal; purchasing software; selecting a new service provider, or changing the way you process or accept payments. If the cardholder data environment changes and the merchant will process cardholder data on the Internet or is using new software, a QSA may be retained to review the new process prior to implementation.

**Training upon hire and annually**

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 “[Annual Policy Acknowledgment Form](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Cardholder_Data_Processing_Agreement.docx?d=w56a9f73d7aff4510837074d7748bb23c)”. IT Directors and designated staff must also comply with [University Computing Security Standards](https://www.umsystem.edu/ums/is/infosec/). The training: Percipio, Saba and Canvas, are all online computer based training that covers PCI as well as other security topics that directly relate to PCI security. <http://www.umsystem.edu/ums/fa/treasurer/training>

**Reporting an Incident**

The Information Security Officer at the respective business unit (<https://www.umsystem.edu/ums/is/infosec/iso>) must be notified immediately of any suspected or real security incidents involving cardholder data:

|  |  |  |
| --- | --- | --- |
| **Contact** | **Organization** | **Phone** |
| Becky Fowler | Chief Information Security Officer, University of Missouri System | 573-882-5182 |
| Bryan Mooney | University of Missouri-Columbia | 573-882-7948 |
| Perry Koob | University of Missouri Science and Technology | 573-341-6398 |
| Justin Malyn | University of Missouri-Kansas City | 816-235-5294 |
| Mark Monroe | University of Missouri-St. Louis | 314-516-4859 |
| Andrew Rodriguez | MU Health System | 573-882-9073 |

* **Preserve the evidence.** 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.

Contact the Information Security Officer at the respective business unit (<https://www.umsystem.edu/ums/is/infosec/iso>) to report any suspected or actual incidents. The Information Security Officer’s phone number should be well known to all employees and should page them during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the Information Security Officer at the respective business unit (<https://www.umsystem.edu/ums/is/infosec/iso>) about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Information Security Officer at the respective business unit (<https://www.umsystem.edu/ums/is/infosec/iso>).

Document any information you know while waiting for the Information Security Officer at the respective business unit (<https://www.umsystem.edu/ums/is/infosec/iso>) to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

**Data Retention**

The [records retention policy](https://www.umsystem.edu/ums/fa/management/records/guide/records-retention-authorization) requires retention of credit card receipts for no less than 2 years. A receipt should only show the last 4 of the customer card. If you are storing full PAN (Primary Account Number) post authorization, you must have your data retention plan approved by Information Security and the Treasurer’s Office. Please see your department’s retention policy or contact [Records Management](https://www.umsystem.edu/ums/fa/management/records/) to determine the type of documents or electronic records required for retention. Please note: the transaction record required by the data retention policy may be the same record needed to defend a customer credit or debit card dispute or chargeback.

**E-mail, scanned (includes Image Now), and other technologies to send cardholder data are prohibited.**

Cardholder data may **NOT** be e-mailed, scanned, stored in Image Now, or sent by end-user messaging technologies by University personnel. If a customer e-mails or sends cardholder data in an unapproved method, the following steps must be taken: (1) notify the customer the transaction cannot be processed; e-mail and other messaging technologies are not secure nor authorized methods to transmit cardholder data (2) request the cardholder data be provided by telephone (3) Delete, “Shift + Delete” the e-mail or, in the case of a fax, cross-cut shred the fax immediately.

**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 analog, dedicated phone line. You must contact the Office or the Treasurer to have your fax machine and connection audited before you can accept fax credit card payments.

**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 complete the [3rd Party Service Provider Checklist](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/3rd_Party_Checklist.docx?d=w1f1f7e4b799e4d28a56643a2c720dfb8) prior to engagement. Service providers must maintain PCI compliance and the department must monitor the annual renewal date of compliance.

**CVV2 validation code or PIN number**

Do not store electronically or on paper the three or four digit CVV or CVV2 validation code on the front or back of a card or the PIN number, personal identification number.

**Mask all except the last four (4) digits of the credit card number**

Terminals, computers, and receipts may display or print no more than the last four digits of the credit card number.

**Forms with 16 digit PAN or credit card numbers**

All internal forms or mail-in forms **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 be cut off and destroyed in a cross-cut shredder. If you are storing full PAN (Primary Account Number) on paper post authorization, you must have your data retention plan approved by Information Security and the Treasurer’s Office. Forms with sixteen-digit card numbers must **NOT** be scanned.

**Data Flow Diagram**

All merchants must have current data flow diagram on file specific to their merchant environment.

* For assistance, contact the Office of the Treasurer

**Physical Inspection of Terminal for Tampering or Substitution**

Merchants must maintain an up-to-date list of all devices. The list must include the following:

* Make, model of device
* Location of the device (for example, the address of the site or facility where the device is located)
* Device serial number or other method of unique identification
* Serial number(s) of the tamper tape that was added to the swipe devices.

Merchants must periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Please see the [Capture Device Periodic Inspection Procedures](https://sharepoint.umsystem.edu/sites/uminfopoint/media/_layouts/15/WopiFrame.aspx?sourcedoc=%7b491CEC72-29DD-43C0-B7EB-CC1E797FB32A%7d&file=Capture_Device_Periodic_Inspection_Procedure.docx&action=default).

**RESOURCES**

**Cardholder Merchant Agreement and Request Form**

***Page 1 of 2***

***Revised: 11/14/2018***

|  |  |
| --- | --- |
| 1. **MERCHANT NAME:**

**24 Character limit on name***The merchant name will print on customers’ monthly statements. It must be a name the customer will recognize.* **MERCHANT NAME***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***MERCHANT NUMBER\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_***(If merchant already exists and you are updating)* | 1. **BUSINESS LOCATION AND CONTACT INFORMATION**
2. Contact Name:
3. Contact e-mail:
4. Phone #:
5. Fax #:
6. Business Address (**24 Character limit)**:
7. City, State, Zip:
 |
| 1. **PCI COMPLIANCE CONTACT (If using the Internet for payment processing, ALSO list IT contact for PCI, Payment Card Industry, compliance.**
2. Contact name:
3. Contact e-mail:
4. Phone #:
 | 1. **ACCOUNTING AND RECONCILING – Person responsible for reconciliation of the account:**
2. Contact name:
3. Contact e-mail:
4. Phone #:
 |
| 1. **INDICATE METHOD OF CREDIT CARD PROCESSING.**
2. Terminal – connected to analog phone line
3. **P2PE** Terminal – IP connection
4. Terminal – Cellular
5. Online – TouchNet hosted
6. Online – TouchNet gateway
7. Online – Authorize.net gateway
8. Other - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 | 1. **INFORMATION ABOUT YOUR BUSINESS**
2. Please indicate if you will be accepting payments for the following services by checking the box. This is important to set up your account for the lowest credit and debit card merchant rates.
3. Accepting flexible spending medical cards?
4. Restaurant accepting tips?
5. Hotel?
 |
| 1. **TERMINAL ORDER**
2. Number of terminals ordered:
3. Terminal Type
4. Chase Ingenico MOVE 5000 **4G** ($399.00)
5. Bluefin **P2PE** PAX A80 ($353.00)
6. Chase DX8000 **4G** ($499.00)
7. Using existing terminal, indicate manufacturer’s name and model:
 | 1. **Information about your Business (cont.)**

1. Approximate annual and average sales  volume:1. Annual Visa/MasterCard sales?
2. Average visa/MasterCard ticket?
3. Annual Discover sales?
4. Average Discover ticket?
5. Services or products you sell?
 |
| 1. **CHARTFIELD INFORMATION AND TERMINAL SETUP:**
2. **REVENUE:**

MO Code: PS ACCOUNT: 1. **FEES:**

MO Code:PS ACCOUNT is 743700 by default1. **TERMINAL SETUP**

Invoice Number, ON or OFF Dial prefix required, YES or NO If YES, what is the dial prefix? \_\_\_\_\_\_Auto Close, YES or NO If YES, what is the auto close time?\_\_\_\_\_\_\_ | 1. **MERCHANT AGREEMENT:**

I have read the [University Credit Card Policy](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Credit_Card_Policy.docx?d=we18ee794de464d918d363432a2e1df5f) and agree to the responsibilities, policies, and procedures established by the Office of the Treasurer. [I am aware of all fees associated with establishing a merchant account and all potential transaction fees. I understand that fees will continue to be assessed until I notify the Treasurer’s Office in writing to cancel the merchant account](http://www.umsystem.edu/ums/fa/treasurer/credit_card_costs). I understand it is my responsibility to supervise the activity of card processors and report to the Office of the Treasurer in writing any breach of cardholder data and to immediately remedy such breach. I also agree to communicate the applicable Payment card Industry (PCI) Data Security Standards (DSS) to my staff and supervise the required annual and system scan, if required. If the cardholder data environment changes after the merchant is established the merchant agrees to have a QSA review the process prior to implementation. **Signature Merchant Contact****\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_****Print name of Merchant Contact****Date:**   |
| ***For use by Office of the Treasurer***Visa/MC/Discover #:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**American Express #:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

***Items of Importance to set up your merchant account:***

* **Questions** – If you have any questions, call John Layman at 573-882-3318 at the Office of the Treasurer. Fax or e-mail this completed form. Fax # 573-882-6595.
* **Phone Line or IP** – To order a phone line to process credit card transactions, contact Telecom at 573-882-5000 (Columbia), Information Technology at 573-341-4357 (MO S&T), Information Technology at 314-516-5000 (UMSL), and Information Services at 816-235-2608 (UMKC).
* **Merchant Account Timeline** – Please allow fifteen (15) business days to set up a merchant account.
* **PCI, Payment Card Industry, Compliance –** The credit and debit card industry formed a council called the Payment Card Industry (PCI) Council which includes Visa, MasterCard, American Express, and Discover. The PCI Council developed Data Security Standards (DSS) to assure consumers that using credit and debit cards are secure. Merchants accepting credit and debit card payments are required to comply with these standards. The applicable security standards depend on the method of processing credit card payments. For more information, please refer to the [University Credit Card Policy](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Credit_Card_Policy.docx?d=we18ee794de464d918d363432a2e1df5f) or contact the Office of the Treasurer.
* **Chart field Information –** Automated journal entries will be made for merchants’ credit and debit card transactions and fees based on the Organization, Fund, and Account number provided. Test transactions should be done when setting up an account or when processing changes are made to your account to insure that automated journal entries are recorded. Also see Reconciliation.
* **Online processing, Software, and Service Providers** – Please contact the Office of the Treasurer for assistance regarding approved methods to process cardholder transactions using online processing, software to process payments, cellular terminals, and contracting with third party PCI service providers.
* [**Credit and Debit Card Fees**](http://www.umsystem.edu/ums/fa/treasurer/credit_card_costs)– There are three types of fees: fees charged by the card brands, transaction fees charged by our Acquiring Bank, Commerce Bank, and, if applicable, fees to process online payments.
1. **Fees charged by the card brands – Visa, MasterCard, American Express, and Discover.**
2. **Visa, MasterCard, and Discover Fees** – approximately 2.0%+ per transaction. Fees are based on the type of credit or debit card presented and are referred to as interchange fees. Generally the rate will be lower for debit card transactions and basic consumer credit card transactions. The rate will be higher for Corporate, Commercial, Reward, Enhanced, World, Foreign and Signature Preferred credit cards as these have reward programs and, therefore, higher fees are charged to the merchant.
3. **American Express Fees** – The American Express rate is a flat rate of 2.3% per transaction.
4. **Transaction processing Fees -** Our Acquiring Bank charges a transaction fee to authorize and settle credit and debit card payments. In addition, they provide statement and transaction information for our merchants.
5. **Internet Online Processing**
6. **Hosted Order Page Rates and Service Providers** – Online service providers charge a one-time set-up fee for the Hosted Order Page and monthly transaction fees.
* **Training on Terminal Processing and Settlement of funds–** Contact Commerce Bank Merchant Services, 800-828-1629, for terminal training. All terminals should be settled at the end of each business day. If you program your terminal to “auto-settle” at the end of a business day, print a settlement report to verify transactions were processed.
* **Reconciliation–** Daily, or at a minimum, monthly reconciliation MUST be completed. Merchant transactions must be reconciled to PeopleSoft to insure deposits are made to the University bank account and to the correct chart field. Monthly statements and daily transaction detail are provided by our Acquiring Bank using an online tool, “My Client Line” (contact the Treasurer’s office, 573-882-3318, to sign up.) Merchants processing using a stand-alone terminal can also obtain daily settlement reports from the terminal.

**Annual Policy Acknowledgment Form**

*Revised 11/14/2018*

**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 read, understand, and follow the provisions in this document, my merchant specific policies and procedures, and the University “[Credit Card Policy](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Credit_Card_Policy.docx?d=we18ee794de464d918d363432a2e1df5f).”

**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](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Inventory_Log.docx?d=w01eea484fe174cd688f377c95f01128f).
	+ Keep a log of my physical inspections using the [capture device periodic inspection log](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Inspection_Log.docx?d=w660489f0bdcc454591f3aa5ea58acaf5).
	+ Place your terminal in a secure location and periodically inspect the terminal for tampering and substitution using the [capture device periodic inspection procedures](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Periodic_Inspection_Procedure.docx?d=w491cec7229dd43c0b7ebcc1e797fb32a).

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

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

Supervisor Signature Supervisor Printed Name Date

**PCI Agreement with Service Providers**

*The following is language to include in agreements with Service Providers involved in transmitting, processing, or storing credit or debit card data to comply with the Payment Card Industry (PCI) Data Security Standards (DSS).*

1. Provisions for Cardholder Data. The provisions set forth in this section apply to service providers including but not limited to, business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data. For purposes of this Section, the term “cardholder data” refers to the number assigned by the card issuer that identifies the cardholder’s account or other cardholder personal information.

1. **<Service providers>** acknowledge in writing to the University that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the University, or to the extent that they could impact the security of the University’s cardholder data environment.
2. **<Service providers>** shall at all times comply with the Payment Card Industry (PCI) Data Security Standards (“PCI DSS”) requirements and is responsible for cardholder data that are prescribed in the PCI Council or the Visa Operating Regulations or otherwise issued by the PCI Council or Visa, as they may be amended from time to time (collectively, the “PCI Requirements”).
3. **<Service providers>** shall detail what specific PCI requirements they manage on behalf of the merchant and what specific PCI requirements are a shared responsibility by the service provider and the university.
4. **<Service provider>** acknowledges and agrees that cardholder data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by the PCI Council or Visa or as required by applicable law.
5. In the event of a breach or intrusion or otherwise unauthorized access to cardholder data stored at or for third party service provider, **<service provider>** shall immediately notify by fax The University Office of the Treasurer, 573-882-6595 and by overnight mail delivered to The Office of the Treasurer at, 118 University Hall, Columbia, MO 65211, and in the manner required in the PCI DSS Requirements, and provide the PCI Council and/or Visa and the acquiring financial institution, our merchant processor, and their respective designees access to third party’s facilities and all pertinent records to conduct a review of third party’s compliance with the PCI Requirements. Third party service provider shall fully cooperate with any reviews of its facilities and records provided for in this paragraph.
6. **<Service provider>** shall maintain appropriate business continuity procedures and systems to ensure security of cardholder data in the event of a disruption, disaster or failure of Merchant’s or third party’s primary data systems.
7. **<Service provider>** and its successors and assigns shall comply with the PCI Requirements after termination of this Agreement.

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

Signature Date

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

Please Print Name Please Print Company Name

**Definitions and Payment Card Industry (PCI) links**

AoC, Attestation of Compliance **–** A report prepared by a QSA in which the QSA and merchant attest to the entity’s compliance status.

Cardholder Data **–** 16-digit PAN (primary account number), Cardholder Name, and Expiration date

CVV Card Verification Value Code (a.k.a CVV2) - This is a three (3) digit number on the back of a credit card. In the case of American Express, this is a four (4) digit code on the front of the credit card.

DSS (Data Security Standards**) –** The credit or debit card data security standards are established by the PCI Council. Merchants at the University must refer to the current and applicable provisions of the DSS. <https://www.pcisecuritystandards.org/security_standards/documents.php>

IP Address – Internet Protocol Address is a unique number used to represent every computer in a network. The format of an IP Address is four sets of numbers separated by dots (e.g. 198.123.123.7)

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.

P2PE – P2PE stands for Point 2 Point Encryption. A validated P2PE solution has been vetted and approved by the council and if installed using the vendor supplied PIM (P2PE Instruction Manual). The following link provides a complete list of validated P2PE solutions. <https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions>

PCI Software - PCI software or PA-DSS software (Payment Application Data Security Standard) is installed on a University computer and determined by the credit card industry to follow the industry’s best practices for securing credit card information. All PA-DSS validated payment applications must be installed per the vendor supplied PA-DSS installation guide. The following link provides a complete list of PCI approved Payment applications. <https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_applications>

PAN (Primary Account Number) – The 16 digit card number.

PED (Pin Entry Device) – Terminal that allows entry of a customer’s Personal Identification Number.

PIN (Personal Identification Number) – Personal number used in debit card transactions.

PCI Council (Payment Card Industry) – Visa, MasterCard, American Express, and Discover, have formed a council to establish Data Security Standards (DSS) for the industry. Please see the following link for their website. <https://www.pcisecuritystandards.org/>

Payment Gateway – A payment gateway is a type of service provider that transmits, processes, or stores credit cardholder data as part of a payment transaction. They facilitate payment transactions such as authorizations and settlement between merchants or processors, also called endpoints. Merchants may send transactions directly to an endpoint or indirectly using a payment gateway.

RoC, Report of Compliance – PCI Report prepared by a Qualified Security Assessor to verify a merchant’s compliance with the PCI DSS, Data Security Standards.

QSA, Qualified Security Assessor – A PCI assessor certified and listed on the PCI Council’s list of QSA companies.

Sensitive Authentication Data - refers to the three (3) or four (4) digit validation code, CVV2, on the front or back of a card and PIN number, personal identification numbers. PCI does not permit this data to be stored even if it is protected according to the PCI Data Security Standards.

Service Provider - A vendor that provides access to the Internet and to applications to facilitate the transfer and/or storage of credit card information. The following link provides a complete list of PCI Compliant Service Providers. (Please note, this list is maintained on Visa’s website.) <http://www.visa.com/splisting/searchGrsp.do>

**Contacts**

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject** | **Office** | **Telephone** | **E-mail** |
| PCI Compliance | Office of the Treasurer | 573-882-3318 | laymanj@umsystem.edu  |
| Data Security – MU, UM, HOSP, & UP | Information Security & Access Management | 573-882-5000 | isam@missouri.edu  |
| Data Security – UMSL  | UMSL IT Security | 314-516-4859 | monroem@umsl.edu  |
| Data Security – MO S&T | MO S&T IT Security | 573-341-6398 | koobp@mst.edu  |
| Data Security – UMKC  | UMKC IT Security | 816-235-5294 | malynj@umkc.edu  |
| Columbia Business PCI Policy | MU Cashiers | 573-882-8227 | carrmm@missouri.edu  |
| UMKC Business PCI Policy | UMKC Cashiers and Collections | 816-235-1366 | SchwartzPN@umkc.edu  |
| MO S&T Business PCI Policy | S&T Cashiers Office | 573-341-7691 | kelleykm@mst.edu  |
| UMSL Business PCI Policy | UMSL Cashiers | 314-516-6608 | hessmr@umsl.edu  |
| UP Business PCI Policy | UP Finance | 573-882-0427 | mckinzier@health.missouri.edu  |
| Hospital Business PCI Policy | Hospital Patient Revenue | 573-882-8874 | smithleann@health.missouri.edu  |
|  | Pharmacies | 573-884-6139 | danaharman@health.missouri.edu  |
|  | Cafeterias & Gift Shops | 573-884-7759 | gebhardtc@health.missouri.edu  |