

Curators of the University of Missouri

<Merchant Name>

Category 1 Merchant

Credit Card Security Policies

PCI DSS 4.0

**CONFIDENTIAL INFORMATION**

This document is the property of Curators of the ; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of the Curators of the .

Revision History

|  |  |  |
| --- | --- | --- |
| Changes | Approving Manager | Date |
| Initial Publication |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Introduction and Scope**

**Introduction**

This document explains Curators of the ’s credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. The Curators of the management is committed to these security policies to protect information utilized by in attaining its business goals. All employees are required to adhere to the policies described within this document.

**Scope of Compliance**

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, **<Merchant>** does not store cardholder data in electronic format, nor does it process or transmit any cardholder data on their systems or premises. Retention of cardholder data, if any, shall be limited to paper reports or receipts.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements for category 1 merchants as defined in the University Credit Card Policy. Should **<Merchant>** implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance as a category 1 merchant, it will be the responsibility of **<Merchant>** to determine the appropriate compliance criteria and implement additional policies and controls as needed. 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.

**Requirement 2: Build and Maintain a Secure Network and Systems**

**Apply Secure Configurations to All System Components**

* Vendor default accounts are managed as follows:
  + If a default vendor default account(s) will be used, the default password is changed per Requirement 8.3.6 (PCI Requirement 2.2.2)
  + If the vendor default accounts(s) will not be used the account is removed or disabled. (PCI Requirement 2.2.2)

**Requirement 3: Protect Stored Account Data**

**Data-retention**

* All security policies and operational procedures that are identified in Requirement 3.x.x are:
  + Documented
  + Kept up to date
  + In use
  + Known to all affected parties. (PCI Requirement 3.1.1)
* Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:
  + Coverage for all locations of stored account data.
  + Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization.
    - This bullet is a best practice until its effective date 03/31/2025
  + Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.
  + Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.
  + Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.
  + A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable. (PCI Requirement 3.2.1)

**Requirement 6: Develop and maintain secure systems and applications.**

**Security Vulnerabilities are Identified and Addressed**

* Security Vulnerabilities are identified and managed as follows:
  + New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
  + Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
  + Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. (PCI Requirement 6.3.1)
* All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:
  + Critical or high-security patches/updates are installed within one month or release. (PCI Requirement 6.3.3)
* All payment page scripts that are loaded and executed in the consumer’s browser are managed as follows:
  + A method is implemented to confirm that each script is authorized.
  + A method is implemented to assure the integrity of each script.
  + An inventory of all scripts is maintained with written justification as to why each is necessary. (PCI Requirement 6.4.3)
    - This bullet is a best practice until its effective date 03/31/2025

**Requirement 8: Identify Users and Authenticate Access to System Components**

**Implement Strong Access Control Measures**

* All users are assigned a unique ID access to system components or cardholder data is allowed. (PCI Requirement 8.2.1)
* Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:
  + Account use is prevented unless needed for an exceptional circumstance.
  + Use is limited to time needed for the exceptional circumstance.
  + Business justification for use is documented.
  + Use is explicitly approved by management.
  + Individual user identity is confirmed before access to an account is granted.
  + Every action taken is attributable to an individual user. (PCI Requirement 8.2.2)
* Access for Terminated user is immediately revoked (PCI Requirement 8.2.5)
* All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
  + Something you know, such as a password or passphrase.
  + Something you have, such as a token device or smart card.
  + Something you are, such as a biometric element. (PCI Requirement 8.3.1)
* If passwords/Passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
  + Set to a unique value for first-time use and upon reset.
  + Forced to be changed immediately after the first use. (PCI Requirement 8.3.5)
* If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:
  + A minimum length of characters (or IF the system does not support 12 characters, a minimum length of eight characters)
  + Contain both numeric and alphabetic characters. (PCI Requirement 8.3.6)
    - This bullet is a best practice until its effective date 03/31/2025
* Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. (PCI Requirement 8.3.7)
* If passwords/passphrases are used as the only authentication factor for user access, then either:
  + Passwords/passphrases are changed at least once every 90 days.

Or

* The security posture of accounts is dynamically analyzed and real-time access to resources is automatically determined accordingly. (PCI Requirement 8.3.9)

**Requirement 9: Restrict Physical Access to Cardholder Data**

**Physically Secure all Media Containing Cardholder Data**

All media with cardholder data is physically secured. (PCI Requirement 9.4.1)

* Offline media backups with cardholder data are stored in a secure location. (PCI Requirement 9.4.1.1)

All media with cardholder data is classified in accordance with the sensitivity of the data. (PCI Requirement 9.4.2)

Media with cardholder data sent outside the facility is secured as follows:

* Media is sent by secured courier or other delivery method that can be accurately tracked. (PCI Requirement 9.4.3)
* Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). (PCI Requirement 9.4.4)

**Destruction of Data**

Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:

* Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
* Materials are stored in secure storage containers prior to destruction. (PCI Requirement 9.4.6)

**Requirement 11: Test Security of Systems and Networks Regularly**

**External Vulnerability Scans and FIM**

* External Vulnerability scans are performed as follows:
  + At least once every three months
  + By PCI SSC Approved Scanning Vendor (ASV)
  + Vulnerabilities are resolved and [*ASV Program Guide*](https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1651609897117) requirements for a passing scan are met
  + Rescans are performed as needed to confirm that vulnerabilities are resolved per the [*ASV Program Guide*](https://www.pcisecuritystandards.org/documents/ASV_Program_Guide_v3.1.pdf?agreement=true&time=1651609897117) requirements for a passing scan. (PCI Requirement 11.3.2)
* External vulnerability scans are performed after any significant change as follows:
  + Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.
  + Rescans are conducted as needed.
  + Scans are performed by qualified personnel and organizational independence of the tester exists. (PCI Requirement 11.3.2.1)
* A change (and tamper) detection mechanism is deployed as follows:
  + To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.
  + The mechanism is configured to evaluate the received HTTP header and payment page.
  + The mechanism functions are performed as follows:
    - At least every seven days

Or

* Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). (PCI Requirement 11.6.1)
  + This bullet is a best practice until its effective date 03/31/2025.

**Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors**

**Incident Response Policy**

The Treasurer’s Office and the Information Security Officers shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI Requirement 12.5.3)

**<Merchant>** has an incident response plan and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:

* Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.
* Incident response procedures with specific containment and mitigation activities for different types of incidents.
* Business recovery and continuity procedures.
* Data backup processes.
* Analysis of legal requirements for reporting compromises.
* Coverage and responses of all critical system components.
* Reference or inclusion of incident response procedures form the payment brands. (PCI Requirement 12.10.1)

**Incident Identification**

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

* Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
* Fraud – Inaccurate information within databases, logs, files or paper record

With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by or under the oversight of the Information Security Officer to assure the integrity of the incident investigation and recovery process. When faced with a potential situation you should do the following:

* **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.

**Reporting an Incident**

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

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 someone 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. (PCI Requirement 12.10.1)

**Root Cause Analysis and Lessons Learned**

Not more than one week following the incident, members of the Information Security Officer at the respective business unit (<https://www.umsystem.edu/ums/is/infosec/iso>) and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly. (PCI Requirement 12.10.1)

**Security Awareness**

**<Merchant>** shall maintain a formal security awareness program is implemented to make all personnel aware of the entities information security policy and procedures, and their role in protecting the cardholder data. (PCI Requirement 12.6.1)

**Service Providers**

**<Merchant>** shall implement and maintain policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows. (PCI Requirement 12.8)

* A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. (PCI Requirement 12.8.1)
* Written agreements with TPSPs are maintained as follows:
  + Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
  + Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity’s CDE. (PCI Requirement 12.8.2)
* **Office of the Treasurer** will complete [the 3rd party check list](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/3rd_Party_Checklist.docx?d=w1f1f7e4b799e4d28a56643a2c720dfb8) whenever a new 3rd party service provider is to be added to the cardholder data environment to ensure proper due diligence. (PCI Requirement 12.8.3)
* A program is implemented to monitor TPSPs’ PCI DSS compliance status at least once every 12 months. (PCI Requirement 12.8.4)
* Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the **<Merchant>.** (PCI Requirement 12.8.5)