

Curators of the University of Missouri

<Merchant Name>

Category 3, 2, and 1 Merchant

Credit Card Security Policies

PCI DSS 4.0

Version - Template

**CONFIDENTIAL INFORMATION**

This document is the property of the Curators of the University of Missouri; 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 University of Missouri.

Revision History

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

**Introduction and Scope**

**Introduction**

This document explains the Curators of the University of Missouri’s credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. The Curators of the University of Missouri management is committed to these security policies to protect information utilized by University of Missouri 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’s>** cardholder environment consists only of PCI-listed approved PTS PIO IP terminals and dial up or cellular terminals, and environment(s) where **<Merchant>** does not store cardholder data in electronic format, nor does it process or transmit any cardholder data on their systems or premises. The environment does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements for category 3, 2, and 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 3, 2, and 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 1: Install and Maintain Network Security Controls**

**Network security controls (NSCs) are configured and maintained.**

**<Merchant>** must have an accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.

**Note:** A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement. (PCI Requirement 1.2.3)

All services, protocols and ports allowed are identified, approved, and have a defined business need. (PCI Requirement 1.2.5)

Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated (PCI Requirement 1.2.6)

Inbound traffic to the CDE is restricted as follows:

* To only traffic that is necessary.
* All other traffic is specifically denied. (PCI Requirement 1.3.1)

Outbound traffic from the CDE is restricted as follows:

* To only traffic that is necessary.
* All other traffic is specifically denied. (PCI Requirement 1.3.2)

NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:

* All wireless traffic from wireless networks into the CDE is denied by default.
* Only wireless traffic with an authorized business purpose is allowed into the CDE. (PCI Requirement 1.3.3)

Anti-spoofing measures are implemented to detect, and block forged source IP addresses from entering the trusted network. (PCI Requirement 1.4.3)

**Requirement 2: Apply Secure Configurations to All System Components**

**System components are configured and managed securely.**

Vendor default accounts are managed as follows:

* If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.
* If the vendor default account(s) will not be used, the account is removed or disabled. (PCI Requirement 2.2.2)

Applicability Notes: This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults.

This requirement also applies where a system component is not installed within an entity’s environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.

All non-console administrative access is encrypted using strong cryptography.

Applicability Notes: This includes administrative access via browser-based interfaces and application programming interfaces (APIs). (PCI Requirement 2.2.7)

For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:

* Default wireless encryption keys.
* Passwords on wireless access points.
* SNMP defaults.
* Any other security-related wireless vendor defaults. (PCI Requirement 2.3.1)

For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:

* Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.
* Whenever a key is suspected of or known to be compromised. PCI Requirement 2.3.2)

**Requirement 3: Protect Stored Cardholder Data**

**Prohibited Data That Cannot be Stored**

All Security Policies and operational procedures that are identified in Requirement 3 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)

SAD (Sensitive Authentication Data) is not retained after authentication, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. (PCI Requirement 3.3.1)

* The full contents of any track data are not retained upon completion od the authorization process.
	+ Track data contents include the following:
		- Cardholder Name.
		- Primary Account Number (PAN).
		- Expiration date.
		- Service Code. (PCI Requirement 3.3.1.1)
* The card verification code (CVV) is not retained upon completion of the authorization process. (PCI Requirement 3.3.1.2)
* The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process. (PCI Requirement 3.3.1.3)

**Displaying PAN**

PAN is masked when displayed (The BIN and the last four digits are the maximum number of digits to be displayed), such that only personnel with legitimate business need can see more than the BIN and last 4 digits of the PAN. (PCI Requirement 3.4.1)

**Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks**

**Transmission of Cardholder Data**

Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:

* Only trusted keys and certificates are accepted.
* Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.
	+ This bullet is a best practice until its 3/31/2024.
		- PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.
* The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.
* The encryption strength is appropriate for the encryption methodology in use. (PCI Requirement 4.2.1)

**Requirement 6: Develop and Maintain Secure Systems and Applications**

**Security Patches**

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 (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of 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 7: Restrict Access to Cardholder Data by Business Need to Know**

**Access to system components and data is appropriately defined and assigned.**

Access is assigned to users, including privileged users, based on:

* Job classification and function
* Least privileges necessary to perform job responsibilities. (PCI Requirement 7.2.2)

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

All security policies and operational procedures that are identified in Requirement 8 are:

* Documented.
* Kept up to date.
* In use.
* Known to all affected parties. (PCI Requirement 8.1.1)

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 the 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)
	+ This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).

Access for Terminated user is immediately revoked (PCI Requirement 8.2.5)

Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:

* Enabled only during the time period needed and disabled when not in use.
* Use is monitored for unexpected activity. (PCI Requirement 8.2.7)
* 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)

MFA is implemented for all remote network access originating from outside the entity’s network that could access or impact the CDE as follows:

* All remote access by all personnel, both users and administrators, originating from outside the entity’s network.
* All remote access by third parties and vendors. (PCI Requirement 8.4.3)

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

**Processes and mechanisms for restricting physical access to cardholder data are defined and understood.**

All security policies and operational procedures that are identified in Requirement 9 are:

* Documented.
* Kept up to date.
* In use.
* Known to all affected parties. (PCI Requirement 9.1.1)

Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. (PCI Requirement 9.2.2)

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)

**Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution**

POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

A [**Capture Device Inventory Log**](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Inventory_Log.docx?d=w01eea484fe174cd688f377c95f01128f) must be kept at every merchant location with a terminal device. All capture devices must be periodically inspected to look for tampering or substitution using the [**Capture Device** **Periodic Inspection Form**.](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Inspection_Log.docx?d=w660489f0bdcc454591f3aa5ea58acaf5)  (PCI Requirement 9.5.1)

The [**Capture Device Inventory Log**](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Inventory_Log.docx?d=w01eea484fe174cd688f377c95f01128f) must contain a list of all devices that capture payment card data (such as card swipe or dip). The Inventory log must contain at the minimum Make, model, location of device, and device serial number (or other method of unique identification). Furthermore, if you have mobile device(s) you must maintain a [**Cellular Terminal Log**](http://umurl.us/CHh7X) detailing who has the device while it is in transit (for every location if applicable). Ensure the list is updated anytime devices are added, relocated or no longer used. (PCI Requirement 9.5.1.1)

**Capture Device Inspection**

All capture devices must be inspected periodically to detect for tampering or substitution using the [**Capture Device Periodic Inspection Form**](https://sharepoint.umsystem.edu/sites/uminfopoint/media/fa/treasurer/credit_cards/Capture_Device_Inspection_Log.docx?d=w660489f0bdcc454591f3aa5ea58acaf5). Furthermore, all relevant personnel must be aware of the procedures for inspecting devices. (PCI Requirement 9.5.1.2)

**Capture Device Security Training**

All relevant personnel must be trained to be aware of attempted tampering or replacement of devices as follows:

* 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). (PCI Requirement 9.5.1.3)

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

External vulnerability scans are performed as follows:

* At least once every three months.
* By a PCI SSC Approved Scanning Vendor (ASV).
* Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met.
* Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide 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)

If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:

* At least once every 12 months and after any changes to segmentation controls/methods.
* Covering all segmentation controls/methods in use.
* Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
* Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).
* Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV). (PCI Requirement 11.4.5)

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: A comprehensive information security policy that governs and provides direction for protection of the entity’s information assets is known and current.**

**Security Policy**

An overall information security policy is:

* Established.
* Published.
* Maintained.
* Disseminated to all relevant personnel, as well as to relevant vendors and business partners. (PCI Requirement 12.1.1)

The information security policy is:

* Reviewed at least once every 12 months.
* Updated as needed to reflect changes to business objectives or risks to the environment. (PCI Requirement 12.1.2)
* The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities. (PCI Requirement 12.1.3)

**Security Responsibilities**

**<Merchant’s>** policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

**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 establish and maintain a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. (PCI Requirement 12.6.1)

**<Merchant>** shall require appropriate staff are trained to be aware of suspicious behavior and to report tampering or substitution of swipe devices. (PCI Requirement 9.5.1.3)

**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)