Credit Card Security Policy
TEC 4.2

Office of Information Technology

Policy Type: Administrative
Applies to: Employees

POLICY DATES

Issued: 2/8/2011
Revised Last: 10/13/2016
Edited by: Tina Stuchell
Reviewed: March 2020

This policy explains the University of Mount Union's credit card security requirements as required by the Payment Card Industry program. University of Mount Union management is committed to these security polices to protect information utilized by the university in attaining its business goals. All employees are required to adhere to the policies described within this document.

University of Mount Union accepts credit cards as payment for a variety of goods and services. By accepting credit cards, University of Mount Union assumes a level of risk with respect to a data breach. In order to manage that risk, credit card transactions processed at the university will comply with the Payment Card Industry Data Security Standards better known as PCI DSS.

As of June 30, 2005, VISA and Master Card Payment Card Industry Security Standards require all entities which handle or store credit cardholder data to comply with a comprehensive set of international security requirements for protecting cardholder data. These standards are designed to protect cardholder data whenever and whatever form it resides in.

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, University of Mount Union's cardholder environment consists only of limited payment applications (typical point of sale systems) connected to the internet, but does not include storage of cardholder data on any computer systems.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in self-assessment questionnaire (SAQ) C.

Table of Contents

Definitions

Term	Definition
PCI DSS	Payment Card Industry Data Security Standard – is a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.
PAN	Acronym for primary account number and also referred to as account number. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account
Untrusted Network	Any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.
Sensitive authentication data	Sensitive authentication data is defined as the following: • The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere). • The card verification code or value (three digit or four digit number printed on the front or back of a payment card. • The personal identification number (PIN) or the encrypted PIN block

Applies to: Employees

Term	Definition

Policy Details

Departments who accept credit cards are responsible to impose and follow procedures that help employees comply with the Payment Card Security Procedures. Each department is responsible to maintain internal controls that prevent payment card breaches and protect sensitive cardholder information. In accepting payment cards, departments acknowledge they are responsible to hire qualified employees, train employees on proper procedures and ensure that employees adhere to these procedures. At no time shall any UMU department electronically retain cardholder data. ANY receipts, reports, etc. shall show only the last four digits of credit card numbers when archived. Selected candidates for positions (including student positions) who have access to processing credit card data must sign a background check and participate in PCI training. Employees are responsible to follow the Payment Card Processing Requirements and this policy. Each employee is responsible to establish and maintain a proper environment of internal controls that prevent credit card security breaches and protect sensitive cardholder information.

Requirement 1: Build and Maintain a Secure Network

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. Access to the internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment. (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.5)
- Firewalls used to protect the cardholder data environment must implement stateful inspection, also known as dynamic packet filtering. (PCI Requirement 1.3.6)

Any mobile and/or employee-owned computers with direct connectivity to the Internet (for example laptops used by employees), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Applies to: Employees

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys
- Passwords
- SNMP Community strings
- Default passwords/passphrases on access points
- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

Configuration standards for all system components must be developed and enforced. University of Mount Union must insure that these standards address all known security vulnerabilities and are consistent with industry accepted system hardening standards. (PCI Requirement 2.2)

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (PCI Requirement 2.2.1)
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system. (PC Requirement 2.2.2)
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure. (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to ensure that security parameter settings set appropriately on all system components before they enter production. (PCI Requirement 2.2.4)

System administrators are responsible to ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI Requirement 2.2.4)

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data:
Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable (PCI Requirement 3.2)

Applies to: Employees

Payment systems must not store sensitive authentication data in any form after authorization (even if encrypted). See definition of sensitive authentication data above under definition. (PCI Requirement 3.2.1, 3.2.2, 3.2.3)

Displaying PAN:
University of Mount Union will mask the display of PANs (Primary account numbers) and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data for example, legal or payment card brand requirements for point of sale (POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: PCI Requirement 3.3)

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

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

Transmission of Cardholder Data
In order to safeguard sensitive cardholder data during transmission over open, public networks, University of Mount Union will use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) These controls will be implemented as follows: (PCI Requirement 4.1)

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. Weak encryption (for example, WEP, SSL version 2.0 or older) is not to be used as a security control for authentication or transmission. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: Use and Regularly Update Anti-Virus Software or Programs

Anti-Virus Protection
All systems particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all known types of malicious software (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, University of Mount Union will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

Requirement 6: Develop and Maintain Secure Systems and Applications

Applies to: Employees

Risk and Vulnerability
University of Mount Union will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as High, Medium or low) to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a high risk to the environment. In addition to the risk ranking, vulnerabilities may be considered critical if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data
Access to University of Mount Union's card holder system components and data is limited to only those individuals whose jobs require such access (PCR Requirement 7.1)

Access limitations must include the following:

- Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)
- Privileges must be assigned to individuals based on job classification and function (also called "role-based" access control. (PCI Requirement 7.1.3)

Requirement 8: Assign a Unique ID to each person with computer access

Remote Access
Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (PCI Requirement 8.3)

Vendor Accounts
All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.1.5)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically secure all areas and media containing cardholder data
All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. (PCI requirement 9.1.2)

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

- All media must be physically secured (PC Requirement 9.5)
- Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.5)
    - Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)
    - Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)

Applies to: Employees

- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

Destruction of Data
All media containing cardholder data must be destroyed when no longer needed for business or legal reasons (PCI Requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI Requirement 9.8.1a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

Protection of Payment Devices
Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted. (PCI Requirement 9.9)

University of Mount Union must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI Requirement 9.9.1)

- Make and model of all devices
- Location of each device (for example: the address of the site or facility where the device is located)
- Device serial number or other method of unique identification

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI Requirement 9.9.2)

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI requirement 9.9.2)

- Employees must 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.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

Requirement 10: Regularly Monitor and Test Networks

Audit log collection
University of Mount Union will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events.

- All actions taken by any individual with root or administrative privileges. (PCI Requirement 10.2.2)
- All invalid logical access attempts (gained logins). (PCI requirement 10.2.4)
- Any use of and changes to identification and authentication mechanisms, including but not limited to creation of new accounts and elevation of privileges, and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI Requirement 10.2.5)

University of Mount Union's log generating and collecting solution will capture the following data elements for the above events:

- User identification (PCI Requirement 10.3.1)
- Type of event (PCI Requirement 10.3.2)
- Date and time (PCI Requirement 10.3.3)
- Success or failure indication. (PCI Requirement 10.3.4)

Applies to: Employees

- Origination of event (PCI Requirement 10.3.5)
- Identify or name of affected data, system component or resource (PCI Requirement 10.3.5)

Audit Log Review
University of Mount Union's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate: (PCI Requirement 10.6.1)

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
- Logs of all critical system components
- Logs of all servers and system components that perform security functions (for example, firewall, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. (PCI Requirement 10.6.2)

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process. (PCI Requirement 10.6.3)

University of Mount Union must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, achieved, or restorable from backup). (PCI Requirement 10.7)

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized wireless access points
At least quarterly, University of Mount Union will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment. (PCI Requirement 11.1)

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components.
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.)
- Wireless devices attached to a network port or network device.

To facilitate the detection process, University of Mount Union will maintain an inventory of authorized wireless access points including a documented business justification. (PCI Requirement 11.1.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the incident response plan (see PCI requirement 12.10). (PCI Requirement 11.1.2)

Vulnerability Scanning
At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), University of Mount Union will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all "high" vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.1)

Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be

Applies to: Employees

performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year (PC Requirement 11.2.2)

For both internal and external vulnerability scans, University of Mount Union shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel. (PCI Requirement 11.2.3)

If segmentation is used to isolate the CDE from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse. 9PCI Requirement 11.3.4)

For all in-scope systems for which it is technically possible, University of Mount Union must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel. (PCI Requirement 11.5.1)

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). (PCI Requirement 11.5)

Requirement 12: Maintain a policy that addresses information security for employees and contractors

Security Policy
University of Mount Union shall establish, publish, and maintain a security policy that addresses how the company will protect data (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1)

See University of Mount Union Information (Data) Security Policy for more details.

Critical Technologies
University of Mount Union shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage (PCI requirement 12.3) See Mount Union's Resource Acceptable Use Policy, Information Data Security Policy, Mobile Device Policy for more details.

These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- Authentication for use of the technology (PCI Requirement 12.3.2
- A list of all such devices and personnel with access (PCI Requirement 12.3.3)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies (PCI Requirement 12.3.6)
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity (PCI Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. (PCI Requirement 12.3.9)

Security Responsibilities

Applies to: Employees

University of Mount Union's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy
VP of Business Affairs and Director of Information Technology 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) See Incident Response Policy.

Incident Identification and Reporting
Employees must be aware of their responsibilities in detecting security incidents and follow the Incident Response Policy. All employees have the responsibility to assist in the reporting of incidents that put data at risk. 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 records.

See the Incident Response Policy for more details. Any suspected or real security incidents involving card holder data should be reported immediately to the VP of Business Affairs, Controller or Director of Information Technology.

Incident Response Policy (PCI Requirement 12.10.1)
Responses can include or proceed through the following stages: identification, severity, classification, containment, eradication, and recovery and root cause analysis resulting in improvement of security controls.

See Incident Response Policy for more details.

Security Awareness
University of Mount Union shall establish and maintain a formal security awareness/training program to make all personnel aware of importance of cardholder data security. (PCI Requirement 12.6)

This policy along with the following policies are important to our PCI compliancy.

- Data Incidence Response Policy
- Information Security Policy

Responsibilities

Position or Office	Responsibilities
Office of Information Technology & Office of Business Affairs	Update of Policy
VPS, Directors, Supervisors, Chairs	Implementation of this policy within their respective units.
Director of IT, VP Business Affairs, Associate VP of Business Affairs, Asst. Director of IT for Technical Services	Oversight of PCI Compliancy security

Credit Card Security Policy
TEC 4.2

Office of Information Technology

Applies to: Employees

Resources

Contacts

Subject	Office	Telephone	E-mail/URL
	Office of Information Technology	330.823.2854	IT@mountunion.edu

History

This policy was established in 2000, last modified in 2011 part of the PCI compliancy efforts and was placed into the new format in 2016.

All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.
Issued: 2/8/2011

Revised: 10/13/2016

Edited:

Reviewed: March 2020