Policy IT014: Credit Card Acceptance and Security Policy

Recommended for Approval by: Fawn L. Petrosky

Fawn Petrosky, Vice President for Finance

Approved by: Dale-Elizabeth Pehrsson

Dr. Dale-Elizabeth Pehrsson, President

Effective Date: 2/24/2023

A. Intent

The intent of this policy is to define the standards for protecting Cardholder Data supplied to the University or any Third-Party Service Provider acting on behalf of the University. Pennsylvania Western University (PennWest) has an obligation to students, vendors, alumni, and others to keep their account information safe when processing credit card payments. All University personnel accepting credit cards for payment of services or goods must protect and secure all credit card data collected, regardless of how it is stored (physically or electronically), including but not limited to account information, card imprints, correspondence, and Terminal Identification Numbers. All department heads and personnel should strictly observe and enforce this policy to ensure that PennWest University customer information and privacy is protected and to assure compliance with the Payment Card Industry Data Security Standard (PCI DSS).

B. Definition(s)

- **PennWest PCI Administration** – Accounting, Information Technology Services, and the Office of Administration and Finance.

- **Cardholder Data** - At a minimum, cardholder data consists of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

- **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.

- **Payment Cards** - For purposes of PCI-DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services,

JCB International, MasterCard Worldwide, or Visa, Inc.

- **PCI** - Acronym for “Payment Card Industry”.
- **PCI DSS** - Acronym for “Payment Card Industry Data Security Standard”.
- **POS** - Acronym for “point of sale.” Hardware and/or software used to process payment card transactions at merchant locations.

C. Policy

Responsibilities under PCI DSS

It is the University’s obligation and the responsibility of each employee who processes Payment Card payments to secure cardholder data and maintain the confidentiality of all Payment Card data as required by PCI-DSS. Only users with a business need to access payment processing systems or cardholder data may do so.

Only approved processing software programs and hardware with secure communication protocols and/or encrypted connections are used for the processing of electronic transactions.

- Departments requesting credit card processing capabilities are required to complete and submit an application to Accounting that includes a business justification.
- Department/staff are NOT to go out and procure their own software as it may have University-wide PCI ramifications.
- Paypal is NOT to be used for University transactions.

It is the responsibility of the Department Director or Lead to:

- Notify Information Technology Services and Accounting of ANY changes to the PCI environment. Changes could be anything from a new employee being hired who can accept credit cards to new card readers being purchased. Any new software capable of accepting payments should be brought to ITS and Accounting for review prior to purchase. Notification of terminated employees who process credit information should be provided immediately so their access can be revoked.
    - You should also update your department documentation when changes occur.
- Verify that all individuals who process credit cards in your area complete required PCI Training annually.
- Limit access to cardholder data to only those individuals who need access.
- Educate employees in your area of this policy and verify that it is followed.
- Maintain internal documented processes and procedures (ie document your process for accepting and processing credit card transactions.) Maintain PCI inventory list. List should include names, roles, and privileges of people who deal with credit cards in your area as well as the PC's and other equipment such as computers, card readers, kiosks, etc. used.
    - Make updates to this documentation as changes occur.
    - You may be periodically asked to provide this information to the PennWest PCI

Administration Team.

- Physically inspect any devices where credit cards can be swiped for signs of tampering.
- Adhere to requirements of the most current PCI DSS. The current version is available at https://www.pcisecuritystandards.org/document_library
- Work with the ITS Information Security team to conduct a PCI assessment no less than annually.

The following Security Best Practices are to be followed:

- Credit card information including PANs (credit card numbers), PIN's, dates, and CVV/CVC codes are NOT to be written on paper or stored electronically.
    - Media are to be destroyed when it is no longer needed for business or legal reasons.
    - NEVER throw paper documents containing credit card or other sensitive information such as social security numbers in the trash! It must be redacted and shredded.
    - Storage containers used for materials that contain sensitive information to be destroyed are to be secured to prevent access to the contents.
- Credit cards shall not be taken over the phone. All transactions should be in person or through a University-approved online processing system.
- Do not accept a credit card that is unsigned, the signatures do not match, or the card appears to be altered or tampered with.
- You may NOT receive or transmit cardholder data via end user messaging technologies (text message, email, social networking services, or instant message) or use API web technology, as all of these practices are considered storage of payment card numbers under PCI-DSS. If you are required to retain a document containing a full credit card number, it must be redacted and promptly cross-cut shredded.
- Once a transaction is processed, all systems and documents containing a PAN shall mask the PAN except for the last 4 digits.
- You may NOT sell, purchase, provide, or exchange credit card information in any form to any third party other than to the University's acquiring bank, depository bank, Visa, MasterCard or other credit card company, or pursuant to a government request.
    - Strict control is to be maintained over internal and external distribution of any kind of media. Media are to be classified according to sensitivity of the data.
- It is strongly discouraged that these documents are mailed even in a redacted form, but if it must be mailed, it must be sent by secured courier or other delivery method that can be accurately tracked.
- You may NOT download credit card information onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.
- Fax transmissions, (both sending and receiving) of credit card and electronic payment information is strongly discouraged. If necessary, transmissions are strictly limited to those fax machines whose access is secured and restricted to authorized individuals only.
- Physical access to offices where Payment Cards are being processed shall be restricted and Payment Card processing devices and cardholder data must be physically secured in a restricted

access area, such as a locked office, using a cable lock, or in a locked cabinet. All media are to be physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes.)

- All transactions must be processed immediately and documents containing cardholder and card information must be shredded.
- A user authentication mechanism is required for access to all payment processing devices using a server or desktop operating system (e.g. Microsoft Windows, Linux, Macintosh OS X, etc.) or mobile operating system (e.g. iOS, Android OS, BlackBerry, etc.).
    - Unique user ID's and strong passwords are to be used. Never share credentials.
    - Report distribution should be controlled and reports physically locked up.
    - Lock your computer (Ctrl+Alt+Delete) when not in front of it.
    - Accounts used by vendors for remote access, support, or maintenance are to be enabled only during the time period needed and disabled when not in use.
- Never process credit card information that has been received by e-mail. Contact the card holder (without forwarding their credit card information back to them) to let them know that their transaction could not be processed from this source and their message has been destroyed to protect their credit card information and direct them to an approved payment method.

Required Action for Theft, Fraud, or Breach

In the event that Cardholder Data is compromised or potentially compromised, immediately contact PennWest Account. This includes lost or stolen files with Cardholder Data, electronic loss of data, databases infected with viruses, loss of paper documents with Cardholder Data and any other loss or potential loss, theft or unauthorized access to devices or payment processing systems. The compromise of any cardholder information should be reported immediately by contacting the Helpdesk by phone at 724-938-5911.

Closing a Credit Card Processing Account

When a Credit Card Processing Account is no longer used, departments must contact Accounting so the Credit Card Processing Account can be closed.

Policy Review

This policy shall be reviewed at least once yearly and updated as necessary to support continued compliance with the then current version of PCI-DSS.

Policy Violations

Violations of this policy shall be reported to PennWest PCI Administration by contacting the Helpdesk at 724-938-5911.

- Failure to comply with this policy may result in any of the following:
    - Suspension or termination of the Payment Card processing privileges for the department;
    - Denial of a request to establish a new Credit Card Processing Account or payment site;

- A departmental charge or series of departmental charges not to exceed the greater of $500 per instance or one-half (1/2) of the total cost of addressing a data breach associated with the violation; and/or
- Administrative action as deemed necessary by the University to prevent a reoccurrence of the violation

D. Procedure(s)

Not applicable.

E. Related policies

Data Classification Policy.

F. Contact Information

Information Technology Services

G. Policy Review Schedule

All policies will be reviewed every two years or on an as needed basis if a change in BOG, PASSHE or Pennsylvania law would create the need for an immediate change.