University Policy

Volume I1: Information Technology	**I1.02.8** **Payment Card Industry Data Standards** **Policy Effective Date:** 06/30/2022 **Last Revised:** 05/30/2023	**Responsible Office:** University Technology Services
Chapter 02: Data Security		**Responsible Officer:** Information Security Officer

POLICY STATEMENT

The Payment Card Industry (PCI) Security Standards Council developed a set of security standards, called Payment Card Information Data Security Standards (PCI DSS), to protect payment card information. These standards govern all merchants and organizations that collect, process, store, or transmit credit card information.

The University is committed to protecting the privacy of payment card information (cardholder information) it processes to comply with the PCI DSS by establishing a policy and a procedure to standardize the process for handling payment card information from the time of payment authorization to completion and ensure that the appropriate controls are in place to safeguard this information against any data breach.

PURPOSE OF THE POLICY

The purpose of this policy is to set out the requirements for safeguarding card holder information that the University processes from a data breach.

WHO IS AFFECTED BY THIS POLICY

All University departments that store, process or transmit credit card information must comply with the PCI DSS requirements. Compliance with PCI DSS also applies to all the University's outsourced payment card processors.

DEFINITIONS

Authorization: For the purpose of a payment card transaction authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

Cardholder - Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

Card Skimmers: Credit card skimmers are devices that criminals attach to ATMs, gas pumps, and any other payment terminals to steal payment card information.

CVC2 – Card Validation Code 2 (MasterCard payment cards): A three or four-digit code that is used to verify the authenticity of a credit card.

CVV2 – Card Verification Value 2 (Visa payment cards): A three or four-digit code that is used to verify the authenticity of a credit card.

CID - Card Identification Number (American Express and Discover payment cards): A three or four-digit code that is used to verify the authenticity of a credit card.

Encryption – Scrambling of information with unreadable data to protect the confidentiality of the actual or real content the information holds.

Merchant: For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services.

Network Segmentation: For the purpose of the PCI DSS, network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not.

P2PE: A PCI Point-to-Point Encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption

PAN (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.

Patch: Update to existing software to add functionality or to correct a defect.

Payment Card: 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.

Payment Application: Any application that stores, processes, or transmits cardholder data as part of authorization or settlement

Payment Card Information/Cardholder Data: At a minimum, this type of data consists of the full PAN and may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code

PIN: (Personal Identification Number): Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provides matches the PIN in the system.

POS (Point of Sale): A hardware and/or software used to process payment card transactions at merchant locations.

SAQ (Self-Assessment Questionnaire): Tool used by any entity to validate its own compliance with the PCI DSS.

Server: Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP.

Subnet: A sub section or segment of a computer network

VLAN (Virtual Local Area Network): Logical local area network that extends beyond a single traditional physical local area network.

REGULATIONS

The Payment Card Industry Data Security Standards (PCI DSS) are made of the following high-level controls that consist of requirements that payment processor merchants must comply with. These controls are designed to secure all payment card information from unauthorized access and apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. To learn more about PCI DSS, visit their website.

Control Description	Requirements
Build and Maintain a Secure Network	*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data
	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	*Requirement 3:* Protect stored cardholder data
	Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	*Requirement 5:* Use and regularly update anti-virus software
	Requirement 6: Develop and maintain secure systems and applications
Implement Strong Access Control Measures	*Requirement 7:* Restrict access to cardholder data by business need-to-know
	Requirement 8: Assign a unique ID to each person with computer access
	Requirement 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	*Requirement 10:* Track and monitor all access to network resources and cardholder data
	Requirement 11: Regularly test security systems and processes
Maintain an Information Security Policy	*Requirement 12:* Maintain a policy that addresses information security

Complying with the PCI DSS

General

- All University departments that operate card payment processes must notify the information security officer prior to using a card payment solution. Only PCI DSS compliant systems must be used for processing card payments and University Technology Services must approve all devices, payment applications, related technology and methods for card payment operations before they are used. Unapproved payment systems must not be used.
- All University departments and employees that handle payment card information for work purposes must comply with the requirements of this policy.
- Only employees who have completed the Information Security Awareness Training and are also trained on PCI DSS requirements may handle cardholder information, and they are responsible for protecting the information from the time of collection to authorization and completion of any payment transaction.
- Employees that handle payment card information may be required to complete further checks in addition to the general background checks for all employees.
- Any suspected or actual incident relating to a breach of payment card information including but not limited to unauthorized disclosure, unsecure transmission, tampering of devices or substitution, impersonation, theft, fraud or any other activity that could negatively impact the cardholder or the University must be reported to the UTS Helpdesk immediately by the University department. University Technology Services will work with the relevant department to investigate the incident following the Information Security Incident Management Policy and Procedure.

- All departments that operate card payment processes are required to complete the relevant PCI DSS Self-Assessment Questionnaire yearly and must satisfy the related requirements to remain compliant with the PCI DSS. In addition, SAQ must be completed for any new payment system/process.

Payment Card Information Usage and Security

- Payment card information must only be used for the purpose for which it has been provided by the cardholder.
- Payment card information such as the primary account number (PAN), end-user pin, 3-digit number at the back known as CVC2, CVV2, or CID must not be stored in any form, digitally (on any computer or University network) or on paper after a payment is authorized.
- The last four digits of the PAN number may be stored for record purposes and audit trail.
- All payment transactions must be approved, and the authorization approval must be retained by the End-user department.
- No point-of-sale solution or device must store PANs, CVC2, CVV2, or CID.
- No point-of-sale solution or device must transmit card payment information in clear text or send information via any unencrypted end-user messaging systems e.g., email or text messages or paper documents such as physical mail.
- Any digital or paper documents with information (No PANs, CVC2, CVV2, or CID) relating to cardholders must be stored in secure areas and only accessible to those who require it for work purposes. Such information must only be retained for the duration required for business purposes following the University's Record Retention Schedule and must be disposed of following the University's Record Disposal Procedure and/or the Electronic Data Erasure Procedure.
- System logs relating to card payment transactions must be stored in a secure location and backed up by following the University's backup process and schedule. Log must not hold any payment card information or other cardholder information that is sensitive.

- The dedicated network must not communicate with other VLANS or subnets on the University's network and must be placed behind a firewall with the appropriate system policies to prevent unauthorized internal network or internet communications.
- The network infrastructure must utilize up-to-date appliances and operating systems, and all payment devices must use vendor-supported operating systems and applications.
- Any modifications or upgrades to the dedicated network that support card payment operations including network configuration, operating systems, appliances and supporting components must follow the UTS change management process and must be approved by the CIO.
- Remote network connection must not be allowed to any card payment devices.

University Managed Payment Card System Security

- Where practical, all devices that are used to process card payments must have antivirus software installed and must be patched regularly to maintain vendor-supported operating systems and applications.
- All default system passwords and other security parameters must be changed and unnecessary default accounts must be removed prior to the system being used.
- Any modifications or upgrades to these devices must follow the UTS change management process and be approved by the CIO.
- Card Readers

- A list of card-reading devices must be maintained along with employees who have access to them.
- The card-reading devices are periodically inspected for tampering or substitution
- Personnel that manage these devices are trained to be aware of suspicious behavior and to report any tampering or substitution of devices. These include but are not limited to:
  - Verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting access to modify or troubleshoot devices
  - Do not install, replace, or return devices without verification
  - Be aware of any suspicious behavior around devices and report any indication of device tampering or substitution to helpdesk@neiu.edu immediately
  - Card readers are locked away when not in use
- An inventory of card-reading devices must be maintained to include
  - Make and model of the devices
  - Location of the devices
  - Device serial number or other methods of unique identification

End-User Responsibility

- All employees who have access to payment card information and supporting computer devices must use a unique ID and password to access the computer devices.
- Passwords for these devices must comply with the University's policy on Strong Passwords.
- Shared user IDs or passwords must not be used to access or operate card payment devices.
- Where practical, lock screens must be enabled on devices used for card payment operations when users are away from the devices.
- All employees who handle payment card information must participate in the annual security awareness training and the PCI DSS training, and formally acknowledge their responsibilities as stated within this policy annually.
- User access must be terminated immediately when it is no longer required or when employment ends. Line managers must notify the system administrator for the payment device and/or UTS to terminate access as applicable.

University Department Responsibilities

- Card Payment Processing Departments:
  - Notify the information security officer to review all new card payment systems. Ensure only approved systems are implemented.
  - Ensure all contract agreements with card payment processors include the requirement for service providers to be PCI DSS compliant and to provide an attestation of compliance statement annually.
  - Liaise with service providers and University Technology Services, to ensure that all vendor-supplied and/or managed computer devices and applications that support or are used to carry out card payment operations are maintained according to the policy requirements.
  - Complete an SAQ annually. Also, complete an SAQ when a new card payment process/system is implemented.

- University Technology Services:
  - Ensure that the network that is dedicated for card payment operations is maintained according to requirements set out in this policy.

- Ensure that all active legacy operating systems, appliances or applications used for card payment operations that are considered to be insecure have complementary security controls in place to protect against any exploitation of inherent vulnerabilities. For example, use secure technologies such as SSH, S-FTP, SSL or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.
- Ensure that antivirus is active on all managed computer devices used for card payment operations.
- Ensure that for computer sessions that are idle for more than 15 minutes, the user is required to re-authenticate to access the terminal or to continue with the session.
- Ensure physical and/or logical controls are in place to restrict access to network jacks.
- Ensure that audit logs are retained for at least one year with a three-month record immediately available for analysis. Where applicable, the audit trail/log should contain the following
  - User identification
  - Type of event
  - Date and time
  - Success or failure indication
  - Origination of event
  - Identity or name of affected data, system components, or resources.
- Ensure that modifications or upgrades to the dedicated network that support card payment operations including network configuration, operating systems, appliances and supporting components follow the UTS change management process and are approved by the CIO.
- Change detection mechanisms are implemented to detect unauthorized modification of critical system files, configuration files, or content files. The change detection mechanism provides alerts to the authorized personnel to investigate. An example of a change detector would be advanced threat protection software.

Vendors

- All contract agreements between the University and vendors/service providers who process card payments on behalf of the University must include a requirement for vendors to comply with the PCI DSS requirements, and each vendor must provide an attestation of compliance report/statement to the University annually.
- In the contract agreements, all service providers must acknowledge the responsibilities for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the University, or to the extent that they could impact the University's cardholder data environment.
- All vendors supplied and managed appliances must comply with the PCI DSS requirements.

Online Transactions (Card Not Present)

- University Technology Services must be informed of all online payment processes.
- All online-payment processors must be PCI DSS compliant.
- No University web payment form must store any card payment information.

PROCEDURES

Procedure for implementing a new card payment system

	Action	Responsibility	Notes
Step 1	Contact the information security officer to discuss the new card payment system to be implemented.	End-user department	Ensure all necessary documents relating to card payment systems are provided. Liaise with the relevant vendors to obtain these documents. This includes information relating to card readers, point of sale applications/computers, related servers, databases, websites, payment gateways, etc.
Step 2	Review card payment systems and approve only PCI DSS compliant systems.	University Technology Services – information security officer	Review all documents provided and liaise with the End-user department and the vendor (if applicable) to obtain any additional information.
Step 3	Determine if a new SAQ or an update to an existing SAQ is required. Ensure SAQ is up-to-date and signed off by the End-user department.	University Technology Services – Information Security Officer and the End-user department	Check any previous SAQ relating to the department. The information security officer will liaise with the End-user department and the vendor to ensure the SAQ is completed and signed off.
Step 4	Approve new card payment systems if they are PCI DSS compliant.	University Technology Services –information security officer	Keep a record of approved devices including make and model of the devices, location of the devices, serial number or other methods of unique identification.
Step 5	Document all completed and approved SAQ along with the information for all card payment systems.	End-user Department/University Technology Services – Information Security Officer	
Additional Requirements		**Responsibility**	**Notes**
Complete an SAQ annually and when a new payment process/system is implemented		Information security officer and the End-user department	This process should begin at least 3 months before the existing SAQ expires or immediately when a new process/system is to be implemented
Request an attestation of compliance statement from vendors annually		End-user departments	End-user departments should keep a copy of all attestation of compliance statements and also send a copy to the information security officer.

GUIDELINES

Training: All training resources are available from the links below:

- Information Security Awareness Training
- PCI DSS Training

Device Inspection: To check for card payment device tampering or substitution:

- Tampering: Check device surfaces to detect tampering for example, addition of card skimmers to devices.
- Substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device) as follows: unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.

AUTHOR REFERENCE

Payment Card Industry Information Security Standard
Baylor University PCI DSS Policy

HISTORY

Completed 30-day public comment on May 30, 2023
Completed 3rd round of internal review on April 7, 2023
Interim Approval June 30, 2022
Draft created June 2022

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Information Security Policy
Acceptable Use Policy
Information Security Awareness Training Policy

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	Email
Vice President for Finance & Administration	*(773) 442-5100*	*vpfinance-admin@neiu.edu*

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for a review. A review will be completed on an annual basis or where there are changes in the PCI DSS requirements necessitating an immediate change to the policy so that it reflects the current requirements. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.