UN Data Security PCI Policy

POLICY CONTENTS

Scope

This policy applies to all university personnel and entities that have access to and electronically transmit cardholder data.

University business units are responsible for following the information security policy development and implementation process established by this policy, communicating their information security policies effectively, reviewing and updating their information security policies regularly, and monitoring their information security policies for compliance and effectiveness.

Policy Statement

PCI DSS Data Security Storage

Cardholder data is not allowed to be stored on the university network, including inside databases; however, there may be a need to store paper copies of cardholder data for small periods of time. Paper copies will not store the cardholder data after authorization.

All personnel and entities associated with the university that intentionally store paper copies of cardholder data are required to seek authorization by contacting the university Bursar's Office or equivalent.

Shared hosting providers for cardholder data systems are not permitted on the university network.

Authorization to store cardholder data does not grant permission to share that data with unauthorized entities.

Transmission of PCI DSS Data Security

Ecommerce solutions and point-of-sale (POS) systems used at the university must meet the PCI DSS requirements. Strong cryptography and security protocols will be utilized to safeguard sensitive data during transmission or on sites redirecting to a third party for transmission of cardholder data. Encryption keys will be protected through the use of validated and recognized certificates by a reputable third party (such as Comodo), so to restrict access to the fewest number of custodians and to be stored in the fewest possible locations.

Risk Reduction and Enforcement

For internally developed solutions, applications must be developed based on industry best practices for secure coding. Some examples of secure coding practices include (but are not limited to) the following:

- Injection flaws
- Buffer overflows
- Insecure cryptographic storage
- Insecure communications
- Improper error handling
- Cross-site scripting
- Improper access control
- Cross-site request forgery
- Broken authentication and session management

In addition, all PCI DSS systems must adhere to the services and vendor default password procedures as defined the PCI DSS Procedures document.

Third party solutions must be certified by the PCI Security Standards Council, and must produce the Attestation of Compliance certificate to the university Bursar's Office or equivalent.

Data scanning software for data loss prevention (DLP) has been installed on the university network to help reduce the risk of data breaches. This device is intended only to flag network traffic and data storage that contains unencrypted regulated data and cardholder data. The information found by the DLP software is strictly used to reduce the risk of regulated data being breached. The use of DLP software complies with NU Executive Memorandum 16.

For public facing web applications redirecting to third party providers to transmit cardholder data, manual or automated application vulnerability security assessments will be performed. Where feasible, a web application firewall will be utilized.

Risk assessments will be performed at least annually and upon significant changes to the CDE, which identifies critical assets, threats, and vulnerabilities.

Training

Training on handling payment cards will be provided at the time authorization is granted to become a university merchant. Training will include (but not limited to):

- Information system security
- Inspection of and recognizing tampering of card swipe devices
- Reporting incidents
- Verifying identities of third-party persons claiming to be repair or maintenance personnel

Training must be completed before accepting payment cards, and annually after that to meet PCI DSS requirements. Records of training will be kept by the department.

University application developers must complete training at least annually on up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.

Policy Enforcement

This policy is enforced by the PCI DSS Task Force. Failure to comply with this policy may result in the loss of the department accepting payment cards and being a merchant of the university.

Reason for Policy

Identity theft continues to rise every year in the United States. The use of the Internet to steal sensitive data such as Social Security Numbers (SSN) and payment card numbers is a major contributor to this rise.

Institutions of higher education have become attractive targets for Internet identity theft. Data credentials such as SSNs are used by thieves to establish fraudulent credit and perform other illegal activities associated with stealing a person's identity. The university has legal and ethical responsibilities to protect this sensitive data. Failure to do so may result in economic or social harm to individuals, loss of the public's confidence in the university's ability to protect sensitive data, and legal liability for damages incurred.

The State of Nebraska approved LB 876, known as the "Consumer Notification of Data Security Breach Act of 2006," in April 2006. This law outlines what must occur if unencrypted data, as defined in the Act, has been breached. In addition, the university must comply with Payment Card Industry (PCI) requirements to properly secure payment card information. Failure to meet these requirements may result in financial penalties and/or loss of ability to process payment cards at the university. As stewards of personal information, the university has a responsibility to be vigilant and proactive in the protection of privacy of campus users and the protection of regulated data that has been entrusted to its care.

The University of Nebraska shall not discriminate based upon age, race, ethnicity, color, national origin, gender-identity, sex, pregnancy, disability, sexual orientation, genetic information, veteran's status, marital status, religion, or political affiliation.

University of Nebraska

Definitions

Regulated Data: University data that is highly confidential and is regulated by state or federal privacy laws. Specific examples of regulated data include:

- Social Security Numbers
- Motor vehicle operator's license number or state identification card number
- Account or credit or debit card numbers, in combination with any required security code, or password that would permit access to a person's financial account
    - Student records (except those defined by university policy as directory information under FERPA)
    - Unique electronic identification number, username, or routing code, in combination with any required security code, access code, or password
    - Unique biometric data such as fingerprint, voice print, retina/iris image, or other unique physical representation Health-related data

Sensitive Data: University data routinely used in conducting business not covered by state or federal privacy laws. The data are protected to preserve the privacy, safety, and reputation of individuals and/ or the university.

Public Data: University data which are categorized as neither "regulated" nor "sensitive." Generally, this is information that can be made available to the public without risk of harm to the university or any entities with an affiliation to the university.

Cardholder Data or CDE: Cardholder data is any personally identifiable information associated with a user of a credit/debit. Primary account number (PAN), name, expiry date, and card verification value 2 (CVV2) are included in this definition.

Related Information

NU Executive Memorandum 16
NU Executive Memorandum 26
University Cash Handling Policy
State of Nebraska Consumer Notification of Data Security Breach Act of 2006

This policy covers the following sections of PCI-DSS 3.2:

- 2.5 Ensure policies and procedures for vendor defaults are documented, in use, and known
- 2.6 Shared hosting providers
- 3.2 Do not store cardholder data after authorization
- 3.5 Document and implement procedures to protect cryptographic keys
- 3.7 Ensure policies and procedures for protected CHD are documented, in use, and known
- 4.1 Use strong cryptography and security protocols
- 4.3 Ensure policies and procedures for encryption are documented, in use, and known
- 6.5 Address common coding vulnerability in software-development processes
- 6.6 Vulnerability security assessment of public facing web applications
- 8.7 Access to any database containing cardholder data is restricted
- 8.8 Ensure policies and procedures for identity and authentication are documented, in use, and known
- 9.9.2 Periodically inspect device surfaces to detect tampering of card swipes
- 9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices
- 12.2 Implement a risk assessment process
- 12.6 Implement a formal security awareness program

History

This policy is a new policy created in 2017.

The University of Nebraska shall not discriminate based upon age, race, ethnicity, color, national origin, gender-identity, sex, pregnancy, disability, sexual orientation, genetic information, veteran's status, marital status, religion, or political affiliation.