FORT HAYS STATE UNIVERSITY
CREDIT CARD SECURITY POLICY

Summary

The Payment Card Industry Data Security Standard (PCI DSS), 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. PCI DSS compliance is mandatory for any organization that collects, processes, or stores credit card information.

Purpose

The purpose of this policy is to establish requirements for collecting, storing, processing and transmitting credit card data to facilitate compliance with the PCI DSS requirements.

Groups Covered

This policy applies to all Fort Hays State University faculty, staff, students, temporary employees and any other persons who collect, process, transmit or store credit card information physically or electronically. Any other entity or individual using FHSU servers or the FHSU network must also abide by this policy. Hereinafter, all applicable persons will be referred to as "Department" for the purposes of this policy.

To help protect against exposure and possible theft of sensitive credit card data and to comply with the PCI DSS requirements, Departments must follow the policies and procedures outlined in this document.

Policy Requirements

Fort Hays State University is required to establish, publish, maintain and disseminate a security policy that addresses all PCI DSS requirements. Each of the 6 goals and 12 requirements as outlined in the PCI DSS are addressed in this document.

Section 1 - 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

Section 2 - Protect Cardholder Data
>Requirement 3: Protect stored cardholder data
>Requirement 4: Encrypt transmission of cardholder data across open, public networks

Section 3 - Maintain a Vulnerability Management Program
>Requirement 5: Use and regularly update anti-virus software
>Requirement 6: Develop and maintain secure systems and applications

Section 4 - 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

Section 5 - 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

Section 6 - Maintain an Information Security Policy
> Requirement 12: Maintain a policy that addresses information security

Policy Implementation

1. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

- All systems used to transmit cardholder data will implement a firewall to guard against intrusion.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

- All system passwords must meet the requirements given in the FHSU Electronic Information Security Policy.

2. Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Web Based Requirements
- In most cases, Departments will be required to use a secure web based gateway or virtual terminal that is supplied by a PCI compliant service provider.
- Credit card data is not entered into a server on the FHSU network.
- The contracted service provider transmits and stores the cardholder data. Data is not retained on any server hosted by the FHSU network.
- Departments will not record, process or store sensitive cardholder data.
- Sensitive authentication data that is stored on gateway systems or virtual terminals is masked and only select information is viewable to designated FHSU Employees with business need-to-know.
- The maximum cardholder data that may be viewed may include the following:
  - The type of payment card (Visa, MasterCard, Discover, American Express)
  - The first four and the last four digits of the primary account number
  - The expiration date

Hard Copy Requirements
- If a Department must physically collect cardholder data for payment, all documents containing sensitive data must be hand-delivered to the Student Fiscal Services office within three business days of collection.
- If hard copy of credit card data is kept by the Department for any length of time before it is delivered to Student Fiscal Services, it must be stored in a secure, locked location with restricted access.

- Only University employees with business need-to-know are allowed to access and/or view the cardholder data.
- Cardholder data will only be stored in the Student Fiscal Services office. Departments are not allowed to permanently retain credit card data.
- Once the credit card data is received in the Student Fiscal Services office, the transaction(s) are processed by a Student Fiscal Services employee on a virtual terminal.
- The hard copy of the credit card data is stored in a secure and locked location restricted from unauthorized access.
- The credit card data will be retained for no more than two fiscal years. The data will be kept for the time period specified for the following purposes:
  - To meet the University's audit requirements.
  - To validate a charge in the event of a cardholder dispute or notification of fraudulent use.
  - To process a credit transaction to the card using the original method of payment.
- At the close of a Fiscal Year end, Student Fiscal Services will dispose of the credit card data stored from the prior Fiscal Year according to Student Fiscal Services Data Retention and Disposal procedures.

Additional Requirements
- It is prohibited to enter or store sensitive authentication data on devices including, but not limited to, office or personal computers, laptops, data storage devices, USB flash drives, DVD's or CD's.
- Credit card data may not be collected or transmitted using unapproved online forms, email, fax or any other unsecured transmission method.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

- No cardholder data shall be transmitted across any data network in plain text. The transmission of cardholder data will require the use of Secure Socket Layer (SSL).

3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

- All computer systems used for handling credit card payments will have current anti-virus software, updated regularly, as outlined in the FHSU Information Assurance Security Policy.

Requirement 6: Develop and maintain secure systems and applications

- All computing systems on the FHSU network and users of computers on the FHSU network must follow and abide by the FHSU Information Assurance Security Policy.

4. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

- Access to physically stored cardholder data and/or any system used to process and store transaction data is restricted and available only to FHSU employees whose job requires access to such information.
- Authorized employees who access cardholder data must have a valid business purpose for doing so.
- Access rights for employees utilizing web-based systems for online transactions are restricted to least privileges necessary to perform job responsibilities.
- The assignment of privileges is based on each employee's job classification and function.

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

- User ID's for all FHSU information systems and services are granted and revoked as per the FHSU Electronic Information Security Policy.
- Creation, access delegation and deletion of user accounts for systems used exclusively for credit card payment purposes is maintained by a system administrator appointed by the FHSU PCI Compliance Team.
  - o Users of such systems are assigned a unique ID and password that allows access to their pre-determined privileges.
  - o The initial password that is provided is changed immediately after the first use.
  - o Users are prompted and required by the system to change passwords at least every 90 days.
  - o Users shall follow good security practices in the selection and use of passwords as per the FHSU Electronic Information Security Policy.
  - o Access for terminated users is immediately revoked and the user ID is disabled.

Requirement 9: Restrict physical access to cardholder data

- Hard copy of credit card data is stored in a separate, secure room within the Student Fiscal Services Cashier office.
- The Cashier's office is accessible only to Student Fiscal Services employees and other University employees who require entrance into the area in order to perform functions of their jobs.
- All access doors to the Cashier area are locked 24 hours a day and entrance is granted by entering an authorization code into a keypad. Only employees of Student Fiscal Services are provided with the pass code(s).
- If a Department must keep hard copy of credit card data for any length of time before it is delivered to Student Fiscal Services, it must be stored in a secure, locked location such as a vault or a locked filing cabinet.
- Only University employees with business need-to-know are allowed to access and/or view the cardholder data.
- When destroying physically stored credit card information, hard copy of cardholder data is cross-shredded by an FHSU employee before it is disposed so that data cannot be reconstructed.

5. **Regularly Monitor and Test Networks**

   Requirement 10: Track and monitor all access to network resources and cardholder data

   - The University will employ network monitoring tools to audit the network activity of systems transmitting cardholder data within the University network.
   - The University will employ intrusion prevention and detection methods to protect the transmission of cardholder data within the University network.

   Requirement 11: Regularly test security systems and processes

   - Vulnerability management will consist of periodic network scans to identify and eliminate security threats that make system and network compromise possible.
   - Processes engaging the network will be reviewed periodically and will be adjusted accordingly as production processes give way to better practices.

6. **Maintain an Information Security Policy**

   Requirement 12: Maintain a policy that addresses information security

   - The FHSU PCI Compliance Team was created to facilitate and maintain compliance with the PCI DSS. The Team consists of members appointed by the Vice President of Administration and Finance. The PCI Compliance Team is responsible for the following:
     o Establish, document and distribute security policies and procedures.
     o Monitor and analyze security alerts and information, and distribute to appropriate personnel.
     o Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
     o Assign responsibility for administering user accounts, including additions, deletions and modifications.
     o Assign responsibility for monitoring and controlling all access to data.

   - All transactions that involve the collection and processing of credit card data at FHSU or on FHSU systems must be performed using methods or systems approved by the University PCI Compliance Team.
   - Departments must obtain approval from the FHSU PCI Compliance Team through an application process before credit card or debit card payments may be accepted.
   - If a Department is approved to accept credit cards, anyone within that Department who will be handling credit card data will attend a mandatory training session that addresses security awareness.

     o Individuals will be required to acknowledge that they have read and understand FHSU's Credit Card Security Policy and Procedures.
   - As an aid to minimize the risk of attacks from internal sources, criminal background checks are performed on each person hired for a position of employment at FHSU as per the policies and procedures relating to criminal background checks for employees.

- Each Department approved to accept credit cards as a form of payment is required to develop internal policy and procedures to help ensure that they are compliant with the PCI DSS requirements.
  - o The policy and corresponding procedures must be submitted to the FHSU PCI Compliance Team for approval.
- The FHSU PCI Compliance Team will monitor and review that the Department is following compliance policies and procedures on at least an annual basis or if non-compliance is suspected.

Risk Assessment

- The PCI Data Security Standard Self Assessment Questionnaire will be completed at least annually to identify threats, vulnerabilities and results.
- The FHSU Credit Card Security Policy will be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

Risk of Non-Compliance

- The requirements in this policy and other FHSU Policies are not optional and will be strongly enforced.
- Failure to comply with the policies and procedures may result in:
  - o Significant fines assessed to the Department and/or FHSU.
  - o Additional costs associated with remediation or legal fees.
  - o Loss of the ability to accept credit cards as a form of payment.
  - o Unfavorable publicity and loss of a positive reputation.

Resources:

PCI Security Standards Council
https://www.pcisecuritystandards.org/

FHSU Electronic Information Security Policy
http://www.fhsu.edu/ctc/FHSU_Information_Assurance_Security_Plan.pdf

Policies and Procedure Relating to Criminal Background Checks for Employees
http://www.fhsu.edu/personnel/background_checks/policies_procedures.pdf

Adopted by President's Cabinet 05/06/09