Administration and Department Payment Card Standard Operating Procedures

Payment Card Industry
Data Security Standard (PCI DSS)
PCI DSS Version 3.2

Rev. 090117

Contents

Purpose

This document and additional supporting documents represents the State University of New York at Fredonia's ("Fredonia") Standard Operating Procedures (SOP) to prevent loss or disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the department and the institution.

PCI DSS

The Payment Card Industry Data Security Standards (PCI DSS) is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all payment card transactions and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council website (https://www.pcisecuritystandards.org).

In order to accept payment card transactions, Fredonia must prove and maintain compliance with the Payment Card Industry Data Security Standards. The Fredonia Payment Card Industry Data Security Standards and additional supporting documents define the requirements for compliant processing, transmitting, storage, and disposal of cardholder data during payment card transactions. These are required in order to reduce the institutional risk associated with the administration of card payments by all departments and to ensure proper internal control and compliance with the PCI DSS.

Visa Cardholder Information Security Plan (CISP)

Visa Inc. instituted the Cardholder Information Security Program (CISP) in June 2001, CISP is intended to protect Visa cardholder data - wherever it resides - ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into the Payment Card Industry Data Security Standard (PCI DSS).

MasterCard Site Data Protection Program (SDP)

The MasterCard Site Data Protection Program, similar to the above Visa CISP, was the original compliance program defining the data security and compliance validation requirements to protect MasterCard payment account data. This program was also incorporated into the PCI DSS when that program was original created.

Scope/Applicability

The Fredonia Payment Card Industry Administration and Department SOP apply to all faculty, staff, students, organizations, affiliates, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of Fredonia. Purchasing Card (aka P-card) data does not fall under the PCI DSS requirements, but shall be protected in a similar manner, particularly as it relates to storage and disposal of cardholder data.

Authority

As a part of that management, the Fredonia PCI DSS Sub-Committee will direct the development and implementation of Fredonia's policies and procedures. The Chairs of the Fredonia Information Security Committee are responsible for enforcement of these procedures as designated by the President.

Standard Operating Procedures

In the course of doing business at Fredonia, including affiliated organizations, it may be necessary for a department or other unit to accept payment cards. Fredonia requires all departments that accept payment cards to do so only in accordance with the Fredonia Payment Card Industry Data Security Standards and the following procedures.

1. Card Acceptance and Handling

The opening of a new merchant account for the purpose of accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of the payment card in that department will be charged to the individual merchant. NOTE: Departments may only use the services of vendors (Third Party Service Providers) which have been approved by PCI DSS Sub-Committee to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order, or internet-based.

1.1. Interested departments or merchants should contact the PCI DSS Sub-Committee to begin the process of accepting payment cards. Steps include:
   1.1.1. Completion of an "Application to become a Merchant Department" and designating a "Merchant Department Responsible Person". Any department accepting payment cards on behalf of the institution or related foundation must designate an individual (Merchant Department Responsible Person) within the department who will have primary authority and responsibility within that department for payment card transactions. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the primary is unavailable.
   1.1.2. Completion of Fredonia PCI DSS Merchant training.
   1.1.3. Review and acknowledgement of the "Fredonia Payment Card Industry Data Security Standards", including proof of ongoing compliance with all requirements of the policy.

1.2. Specific details regarding processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Merchants are responsible for the reconciliation of any associated accounts on an ongoing basis.

1.3. All service providers and third party vendors providing payment card services must be PCI DSS compliant. Departments who contract with third-party service providers must maintain a list that documents all service providers and:
   1.3.1. Ensure contracts include language stating that the service provider or third party vendor is PCI compliant and will protect all cardholder data.
   1.3.2. Annually audit and obtain an Attestation of PCI Compliance (AoC) from all service providers and third-party vendors. A lapse in PCI compliance could result in the termination of the relationship.

2. Payment Card Data Security

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

PROCESSING AND COLLECTION

1.1. Access to cardholder data (CHD) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD and review the list periodically to ensure that the list reflects the most current access needed and granted.

1.2. Equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:

1.2.1. Maintaining an inventory/list of devices and their location;

1.2.2. Periodically inspecting the devices to check for tampering or substitution;

1.2.3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.

1.3. Email must never be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined below is critical. If payment card data is received in an email then:

1.3.1. The email should be replied to immediately with the payment card number deleted stating that "Fredonia does not accept payment card data via email as it is not a secure method of transmitting cardholder data".

1.3.2. Provide a list of the alternate, compliant option(s) for payment.

1.3.3. Delete the email from your inbox and also delete it from your email Trash.

1.4. The use of fax machines to transmit payment card information to a merchant department is strictly prohibited.

STORAGE AND DESTRUCTION

1.5. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.

1.6. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data.

1.7. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card validation code.

1.8. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

1.9. Merchants must refrain from retaining Cardholder data. CHD must be destroyed immediately using a PCI DSS-approved method of destruction. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept..

3. Risk Assessment

Implement a formal risk assessment process in which current threats and vulnerabilities to the institution's network and processing environment, including staff, are analyzed. Risk assessments must be conducted annually. Information Technology should conduct the risk assessment of the infrastructure and threats; departments that accept payment cards should also conduct an assessment of their physical environments and assess risks to the payment environment. Address all threats with mitigation tasks, timelines and/or acceptance statements. Prepare and maintain documented output from the risk assessment exercise(s).

4. Incident Response

In the event of a breach or suspected breach of security, the department or unit must immediately execute the Fredonia Payment Card Incident Response Plan. The plan must include notifications, staff requirements, and handling procedures. If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify the Information Security Office at (716) 673-4725. The Incident Response Plan should be reviewed and tested at least annually.

5. Policy and Training

Ensure policy and procedure documentation governing cardholder data exists and that it covers the entirety of the PCI DSS. Document users' acknowledgement of understanding and compliance with all policies and procedures annually. Ensure training on the PCI DSS and overall information security is provided to all staff members with access to cardholder data and/or the processing environment upon hire, and at least annually thereafter.

6. Sanctions

Failure to meet the requirements outlined in the Fredonia Payment Card Industry Standard and this procedure will result in suspension of the physical and, if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation the payment card brands may assess penalties to the Merchant's bank which will likely then be passed on to Fredonia. Any fines and assessments imposed will be the responsibility of the impacted division. A one-time penalty of up to $500,000 per card brand per breach can be assessed as well as on-going monthly penalties.

Persons in violation of this policy and procedure are subject to sanctions, including the potential loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state, or federal laws. The Fredonia PCI DSS Sub-Committee will carry out its responsibility to report such violations to the appropriate authorities.

Interpretations

The authority to interpret these procedures rests with the State University of New York at Fredonia President and the President's Cabinet.

Glossary

Term	Definition
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
Cardholder Data (CHD)	At a minimum, cardholder data consists of the full 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.
Cardholder Data Environment (CDE)	The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
Disposal	CHD must be disposed of in a certain manner that renders all data unrecoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, and USB storage devices. Before disposal or repurposing, computer drives should be sanitized in accordance with Information Management and Cyber Security Policy. The approved disposal methods are: ● Cross-cut shredding, Incineration, Approved shredding or disposal service
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by Fredonia to accept payment cards and has been assigned a Merchant identification number.
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the five major payment card brands: ● Visa, MasterCard, American Express, Discover, JCB
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Affiliate	Any entity that utilizes the State University of New York at Fredonia's electronic services or computing infrastructure with a legitimate business purpose to process credit card payments.