Payment Card Industry - Data Security Standards

Background

Since the State University of New York at Fredonia ("Fredonia") and related affiliates currently accept credit cards as a reliable and secure means of payment for services and products, Fredonia is required to obtain and maintain PCI-DSS compliance for each credit card processing entity ("merchant") across campus. The Payment Card Industry Data Security Standards (PCI - DSS) is a mandated information security standard for organizations that store, process, access or transmit cardholder data (CHD or credit card numbers) in any format (e.g. electronic, paper-based, etc). A data security breach that stems from a gap in PCI compliance is, by definition, a breach of the contract between the merchant and the card brands. Consequences for having a breach of cardholder data include substantial fines up to $500,000 (per card brand) as well as forensic costs and reparation for the fraudulent transactions.

Purpose

This standard is intended to prevent the loss or disclosure of customer information including credit card numbers. 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 unit and Fredonia.

Standard

It is Fredonia's standard to allow acceptance of credit cards as a form of payment for goods and services. Fredonia requires all departments that accept credit cards to do so only in compliance with credit card industry standards and in accordance with the procedures outlined in this document and other established requirements.

Roles and Responsibilities

The path to obtaining and retaining PCI-DSS compliance is complex and can not effectively be achieved without a strong partnership between all parties responsible for the various activities and components. Although the Division of Finance and Administration together with Academic Affairs - Information Technology Services (ITS) take a joint role and joint responsibility in leading Fredonia's PCI-DSS compliance effort, all campus entities are responsible for adhering to all aspects of PCI-DSS compliance .

Academic Affairs - Information Technology and Services (ITS) responsibilities include:

- Recommend, install, and maintain all information technology systems and services used in the storage, processing, transmission of, and access to credit card information. This includes all networks, card swipe devices, computer systems, network segments, firewalls, etc. used in the processing of credit cards.
- Develop and implement a service offering that includes the technology and support to achieve and maintain PCI-DSS compliance while minimizing PCI-DSS scope and associated costs.
- Investigate new, more secure, and less intrusive technologies used in the processing of credit card transactions and make recommendations to Finance and Administration and other Business Partners when said technologies exist and may be adoptable by Fredonia.

Finance and Administration's responsibilities include:

- Draft and follow documented business practices and procedures outlining how credit cards are taken and processed at Fredonia.
- Set PCI-DSS processing standards including who is allowed to take credit cards as a form of payment at Fredonia and outline how such processes will be constructed.
- Enforce best practices on how credit cards are processed and who has the authority to take credit cards as a form of payment at Fredonia.

Finance and Administration and ITS joint responsibilities include:

- Co-chair the campus effort of drafting the PCI-DSS compliance project plan that defines the steps required to ensure the University becomes and maintains PCI-DSS compliance.
- Devise training schedules, review training materials, assist in the delivery of training sessions (via Fredonia staff or assisting with coordinating with external consultant).
- Develop strategies for achieving and maintaining PCI-DSS compliance for on-campus merchants who have complex business processes.
- Monitor, support, and communicate with merchant areas to ensure any and all corrective actions are properly applied in a timely manner.
- Attend conferences and workshops as to maintain a modern, working knowledge of PCI-DSS compliance efforts throughout higher education.

Merchant Department Responsible Person (MDRP) responsibilities include:

- Comply with the Fredonia Payment Card Industry - Data Security Standards (PCI-DSS).
- Attend the required PCI-DSS Merchant Annual Training.
- Report any security incidents to the Information Security Office.

- Communicate on an on-going basis of any changes within their departmental procedures and practices as they relate to PCI-DSS compliance.

Information Security Committee:

- The Information Security Committee co-chairs are responsible for the enforcement of this standard and related procedures.
- The Information Security Committee co-chairs will have the Cabinet level authority to prohibit credit card processing for campus community and University departments in the event they are found to be non-compliant.

PCI-DSS Sub-Committee:

- The PCI-DSS sub-committee will be responsible for the on-going compliance reviews, projects and initiatives required for Fredonia (and related affiliates) to maintain PCI-DSS compliance.
- The PCI-DSS sub-committee will report to the Information Security Committee and be co-chaired by the Vice President of Finance and Administration's designee and the Information Security Officer.
- The PCI-DSS sub-committee will provide updates and make recommendations to the Information Security Committee as to the status of compliance efforts.
- Campus community merchants representing other Fredonia divisions and affiliates (e.g. Research Foundation, etc.) will be requested to attend committee meetings and trainings as needed.

Sub-Committee Membership:

Title	**Division or Affiliate**
Information Security Officer	Academic Affairs - Information Technology Services
Director of Information Technology	Faculty Student Association
Associate Vice President of Information Technology & Chief Information Officer	Academic Affairs - Information Technology Services
Director of Student Accounts	Finance and Administration
Director of Internal Control	Finance and Administration

Scope

The Fredonia Payment Card Industry-Data Security Standards (PCI-DSS) apply to all faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with credit card handling. This includes transmission, storage and/or processing of credit card numbers, in any form (electronic or paper), on behalf of Fredonia or a Fredonia affiliate.

Authority

The President's Cabinet has delegated their authority to enforce this standard to the Co-Chairs of the Information Security Committee.

Glossary

Term	Definition
Payment Card Industry Data Security Standards (PCI-DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: Visa, MasterCard, American Express, Discover, JCB
Card Brands	Visa, MasterCard, American Express, Discover, JCB
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a credit card.
Card Holder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit 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.
Cardholder Name	The name of the Cardholder to whom the card has been issued.

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.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of credit 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.
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.
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.
PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with applicable Fredonia policies. The approved disposal methods include the following: Cross-cut shredding, Incineration, Approved shredding or an

	approved (physical or electronic) contracted disposal service.
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept credit cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions. This individual is typically the department Director or Chairperson.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.