Payment Cardholder Data Handling Procedures (required to accept any credit card payments)

Introduction:

The Procedures that follow will allow the University to maintain its compliance with the Payment Card Industry (PCI) Data Security Standard. The University must follow this Standard and procedures in order to maintain its ability to accept credit/debit cards for payment for goods and services. Those involved in the processing of cardholder data must ensure that business practices comply with the security standards outlined in this document.

Failure to comply with these procedures by one area of the University, may result in the entire University losing its ability to accept credit cards. Universal compliance is, therefore, extremely important.

For assistance with these procedures please contact PCI Compliance Officer (Business Operations, Financial Services).

Overview:

These standards apply to all forms of cardholder data and sensitive authentication data as defined by the Payment Card Industry Data Security Standard including:

- Primary Account Number
- Cardholder Name
- Expiration Date
- Service Code
- Full magnetic stripe data or equivalent data on a chip
- Card verification data (CAV2/CVC2/CVV2/CID)
- PINs/PIN blocks

Definitions:

1. CVV Number – The CVV (Card Verification Value) or CVN (Card Verification Number) or CID (Card Identification Number) is the three-digit (or four-digit on AmEx) security code that is printed on the back of a credit card. This number is never transferred during card swipes and should only be known by the cardholder (or the person holding the card in their hand).
2. Electronic Commerce – commonly known as e-commerce and consists of the buying and selling of products or services over electronic systems such as the internet.
3. PCI-DSS – Payment Card Industry – Data Security Standard is a standard developed by the PCI Security Standards Council to protect against fraud in credit card transactions.
4. Payment Processor – Third-party merchant services provider who acts as an intermediary between merchants, credit card issuers (Visa, etc.) and merchant account providers.
5. Payment Gateway – The service that automates the payment transaction between the merchant and buyer. It is usually a third-party service that processes, verifies and accepts or declines card transactions on behalf of the merchant, via secure internet connections.
6. Supporting documentation – Includes receipts, invoices, and other records containing partial card numbers. Retain these documents for seven years as required by Canada Revenue Agency.

7. Valid business purpose – Documents should be kept for 18 months in order to respond to disputes. This is a function of our relationship with respect to chargebacks and Chase Paymentech.

Procedures:

1.0 Accountability

Merchants are responsible for:

- The ongoing protection of cardholder data for the purpose of processing and storage.
- Adherence to the standards and directives outlined in this document.
- Ensuring that safeguards designed to protect cardholder data are not tampered with or modified.
- Ensuring the merchant account information (including user account passwords for online credit card processing) is properly protected.
- Complete annual PCI self-assessment questionnaires to accurately reflect practices.
- Follow the Cardholder Data Security Incident Response Plan when a breach or suspected breach has occurred.
- Attend annual training on cardholder data protection standards and practices.
- Ensuring that appropriate background checks have been performed prior to hiring of any positions with access to cardholder information.

The PCI Compliance Team and Business Operations are responsible for:

- Ensuring that merchants are provided access to training materials that outline their responsibilities for protecting cardholder data.
- Actively promoting the awareness of security risks associated with processing and storing cardholder data.
- Ensuring that controls are appropriately designed and put in place to safeguard cardholder data.
- Setting technical, physical, and procedural security standards to protect sensitive data.
- The institution’s compliance with the Payment Card Industry Data Security Standard.

2.0 Merchant Authorization

All merchants must be authorized by Business Operations, Financial Services.

Employees must be trained in the proper handling of credit and debit card information. Individuals who are new to the role must be trained prior to processing cardholder data.

Any changes to business processes involving credit cards should be done in consultation with and vetted by Business Operations.

3.0 Collection of Cardholder Data

This section must be followed in conjunction with the next section, Storage and Access of Cardholder Data.

The preferred procedure to collect cardholder data (i.e. process credit card transactions) is:

- Using face-to-face (Chip & PIN) transactions (where the customer is present using a credit card machine), or
- Using the University's outsourced ecommerce solution for online stores.

In accordance with the University's Cash/Cash Equivalent Handling policy, web-based payments must be processed using a PCI-compliant service provider approved by Business Operations.

Collecting cardholder data where the 'Cardholder is Not Present' (other than via the approved ecommerce solution) may only be done with the formal consent of Business Operations. For "Cardholder not Present" transactions, card details must be collected by phone, and the order taker must enter the card transaction directly into the card terminal. Only the data outlined in the chart under Section 4.0 may be collected.

The following processes are strictly prohibited in the collection of cardholder data:
- Cardholder data must not be collected via email. Merchants may not request that customers submit cardholder information via email or other insecure means.
- A merchant may not ask a recipient to write down his/her CVV or PIN on paper forms.
- Using an unauthorized ecommerce solution.
- The use of fax to collect cardholder data is not allowed.
- The use of a telephone for cardholder data collection is strongly discouraged. If there's a business need to collect cardholder data over the phone, strict guidelines must be adhered to.

3.1 Use of Telephone

The use of telephones for the collection of cardholder data is strongly discouraged. If a business unit must use telephones in the data collection process, the following standards must be followed:

- Business unit managers must ensure that all personnel are aware of the specific protocols associated with using a telephone to collect cardholder data.
- Telephone numbers used by customers in the collection of cardholder data MUST NOT employ any type of voice recording technology such as voicemail or call quality systems.
- Employees must never set up call to another VoIP extension or external number (e.g. cell phone).
- Calls must be received using an appropriately configured Carleton VoIP phone extension. The Carleton University VoIP telephone system employs controls such as encryption of voice traffic and logical segmentation from other IP networks to secure sensitive voice data.
- Card authentication data (e.g. CVV, CVC, CID2, PIN) must not be retained after the transaction has been authorized.

4.0 Storage and Access of Cardholder Data

	Data Element	Storage Permitted	Render Stored Account Data **Unreadable**
Cardholder data	Primary account number (PAN)	Yes	Yes
	Cardholder name	Yes	No
	Expiration date	Yes	No
Sensitive authentication data	Full magnetic stripe	No	Cannot Store
	CVC2/CVV2/CID	No	Cannot Store After Authorization
	PIN / PIN block	No	Cannot Store

Additionally, any storage of cardholder data must comply with the following protocols:

- Physical copies of cardholder data (e.g. customer receipts, merchant duplicate receipts, reports, etc.) should be retained only as long as there is a valid business reason to do so.
- On physical documents no more than the first 6 and last 4 digits of the Primary Account Number should be displayed. All other elements of the card number must be masked.
- Any cardholder data in physical hardcopy will be physically secured in a locked drawer, locked room, or locked filing cabinet. The merchant must collect keys from any individual who leaves the University or whose responsibilities no longer require access such cardholder data. If combination locks are used to protect cardholder data, the combination must be changed when an individual who knows the combination leaves the University or no longer requires access.
- Cardholder data must not be stored in electronic format (e.g. servers, portable devices such as a laptop, PDA, flash drive, etc.)
- An inventory and inventory log of all media containing cardholder data must be maintained. The inventory should be reviewed at least annually.
- Access to cardholder data must be restricted appropriately based on job function.
- Access to facilities where cardholder data is stored must be logged.
- Unauthorized personnel must be escorted at all times in areas where credit card data is being processed.

5.0 Destruction of Cardholder data

As noted in Section 4, for Cardholder not Present transactions, the following customer card data must not be retained by University personnel, and must be destroyed, immediately after processing the card transaction:

- Card verification data (CAV2/CVC2/CVV2/CID)

All other cardholder data must be destroyed after it is no longer necessary for business purposes. A process must be in place in merchant departments to ensure that the cardholder data is destroyed in a timely manner, including a quarterly review to ensure all data no longer required has been destroyed.

Cross shredders and Iron Mountain shredding boxes must be used to destroy designated forms containing cardholder data and sensitive authentication data.

6.0 Movement, Distribution and Transmission of cardholder data

Management must approve the movement of cardholder data by a third party. When physically transporting credit card data to a 3rd party entity, the cardholder data must be in an envelope marked “Confidential” and sent by a trusted courier. Tracking data must be maintained for any packages containing cardholder data.

Cardholder data must never be transmitted to/from Merchants using traditional messaging technologies including email, instant messaging, SMS.

7.0 Response to Security Incidents Involving Cardholder Data

In the event that any malicious attempt, either successful or unsuccessful, by an unauthorized party to negatively impact the confidentiality or integrity of cardholder data is detected, the merchant must initiate the Cardholder Data Security Incident Response Plan (available on Financial Services website).

8.0 Use of Credit Card Processing Terminals

Credit/debit card processing machines must be configured to display only the last four digits of a credit card number on printed receipts.

Credit/debit card processing machines and point of sale terminals must be configured to not store either the full contents of any track for the magnetic strip, nor the three-digit card validation code, nor any card authentication data (e.g. PIN/PIN block)

Merchants, who input card information directly into a web-based payment application on behalf of the cardholder, must use a dedicated workstation on a PCI-compliant network connection (a virtual terminal device).

In accordance with PCI DSS requirements, networks and systems used in the collection and processing of cardholder data will be subject to quarterly vulnerability scans.

9.0 Virtual Terminals

Some merchants will be required to use a computer terminal (virtual terminal) to enter transactions directly to the card processing company’s website. In these cases, the following standards must be followed:

- A dedicated, single-purpose workstation must be used.

- Virtual terminals must not be connected to the CUNET environment; however, they must employ a similar level of security controls found in the CUNET environment.
- Virtual terminals must be connected to the network using a segmented VLAN that is logically segregated from the rest of the network. Unique private IP addresses will be assigned to each virtual terminal located on the segmented network.
- Virtual terminals will employ a separate DNS view from the rest of campus.
- Employees must use an authorized workstation to process virtual terminal transactions. ITS Security will assess whether virtual terminals are appropriately configured.
- Appropriate configuration of virtual terminals includes:
    - Automated patching
    - Restrictive firewalling
    - PCI compliant antivirus solution
    - Removal of any unnecessary software/services
    - Disabled USB
    - Remote access disabled
    - Appropriate logging
- Virtual terminals must be physically secured and must not be located in a publicly accessible area
- Unique user accounts must be configured and must employ a password policy that aligns with ITS' password policy for information systems.