Hinsdale Public Library
PCI Security Policy

Purpose

The purpose of this policy is to establish guidelines for processing payments with credit/debit cards at the Hinsdale Public Library's (HPL) Point of Sale (POS) terminal. These guidelines are developed in compliance with the Payment Card Industry Data Security Standard (PCI-DSS).

Terms

Cardholder Data: At a minimum, cardholder data consists of the full primary account number (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.

DSS: Acronym for "Data Security Standard" and also referred to as "PCI DSS."

Firewall Access Rules: These rules control a network device's ability to send traffic to or receive traffic from programs, system services, computers, or users.

Information Security: Protection of information to insure confidentiality, integrity, and availability.

Network Segregation: Developing and enforcing a rule set controlling which computing devices are permitted to communicate with other identified computing devices.

PAN: Acronym for "primary account number" (or "account number"). This is a unique payment card number (typically for credit or debit cards) that identifies the issuer.

PCI: Acronym for "Payment Card Industry."

POS: Acronym for "Point of Sale."

Guidelines

a. This policy applies to all HPL employees and to contractors and consultants who have access to the cardholder data environment.
b. All employees who have access to cardholder data must receive security awareness training and acknowledge that they have read and understand HPL's PCI Security Policy. This policy will be reviewed with applicable staff annually.
c. HPL uses a POS terminal connected to the Internet. The terminal is isolated from all of the other computer systems in the library and properly secured by means of firewall access rules and network segregation.
d. HPL does not accept payments via telephone.
e. No cardholder data is entered or stored in any HPL computer system.
f. Cardholder data may not be transmitted via email.
g. No cardholder data will be written down.

No more than the last four digits of a PAN shall be printed on either the HPL copy or the customer copy of any receipts or reports.

Hinsdale Public Library
PCI Security Policy

Responsibility

HPL trains staff on its PCI Security Policy. Any employee found to have violated this policy may be subject to disciplinary action as identified in the Library's Personnel Policy.

a. HPL does not share cardholder information with other companies or third parties.
b. Access to cardholder data shall be limited only to those individuals whose job requires such access and shall be restricted to a "need to know" basis.
c. Distribution and storage of cardholder data are controlled by the Patron Service Manager and Office Manager. Receipts and reports containing cardholder data are secured until they are delivered to the Office Manager.
d. No HPL employee will divulge, copy, release, sell, loan, review, alter or destroy any information except as properly authorized.
e. Employees protect confidential information wherever it is located, e.g., held on physical documents, communicated over voice or data networks, exchanged in conversation, etc.

Credit Card Incident Reporting
Instructions for reporting suspected credit card fraud or interference and the HPL's response are detailed in the HPL Emergency Manual.

Records
a. HPL retains receipts and reports containing cardholder data in a secure location until they are eligible for disposal.
b. Eligibility for disposal is determined under the Illinois Local Records Act.
c. Eligible records are destroyed onsite.

Service Providers
HPL maintains and implements procedures to manage service providers with whom cardholder data is shared. HPL:
a. Maintains a list of service providers.
b. Maintains a written agreement with service providers, including acknowledgement that the service providers are responsible for the security of cardholder data they possess, store, process, or transmit on behalf of the customer.
c. Establishes a service provider's ability to meet these criteria before entering into an agreement with them.
d. Monitors service providers' PCI DSS compliance status at least annually.
e. Maintains information about which PCI DSS requirements are managed by each service provider.

Compliance Schedule

MINIMUM FREQUENCY	DESCRIPTION
As Needed	• Track and monitor vendor access to Library systems • Complete Change Management Audit Form
Monthly	• Review firewall reports to verify that any unauthorized access has been halted or obtain documentation from the vendor that the HPL's ports are being monitored.

Quarterly	• Use auditing and monitoring tools to verify that:
	  ○ All prohibited inbound and outbound traffic is denied
	  ○ All router configuration files are secure and synchronized
	• Verify that perimeter firewalls between all wireless networks are configured correctly
	• Use a wireless analyzer to establish the validity of each wireless network that appears on the analyzer
	• Verify all daily operations are being performed. Verify (for a sample of days) that the tracking mechanism has successfully recorded completion of all tasks.

Semi-annually (Sample all users until completed)	• Verify that the firewall software on personal computers is installed and active for a sample of users. Rotate the sample so that all user mobile computers are reviewed every six months.
Annually	• Review the PCI Security Policy annually and update as needed • Review relevant contracts to confirm that service providers acknowledge responsibility for protecting cardholder data

Firewall and networking systems provide Intrusion Detection Services (IDS) with alerts in real time. HPL's IT staff investigate all alerts.

References

https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-B_IP.pdf

Hinsdale Public Library Board of Trustees
Approved and Adopted by Library Board on 08/28/2012.
Rev 01/26/2016, 01/24/17, 02/19/19/ 01/21/20, 3/22/22, 09/26/23.

Hinsdale Public Library
PCI Security Policy

Instructions for filling out the Rogue Wireless Access Point & Network Security Incident Form

This form will be filled out when a staff member finds a Wireless Access Point, system or any device that is not owned by HPL plugged into the Library's network. The incident should be immediately reported to the IT Manager and Person in Charge.

Staff Member's Name:

Staff Member's Department:

Date of Discovery:

Time of Discovery:

Location where the equipment was found:

As detailed a description as possible:

Owner's information, if known:

If applicable, identify where the equipment was plugged into one of the Library's data wall/floor jacks:

Include all known system information:

Describe the physical security of the location where the equipment was found. For example, "Teen Lounge – no physical security" or "Server Room – Locked door, only accessible with inside key/authorized key card."

Submit completed form to IT Manager within 24 hours of the incident.

Change Management Audit Form

To be completed by the IT Manager when relevant PCI changes are made to the Network, Security or Firewall settings, or the vulnerability scanning process. Results to be shared with the Executive Director.

What significant change has been made:

Purpose of the change:

When was it made:

Who authorized the change:

Who made the change; what third parties were involved:

Who validated the change:

What are the impacts and results of the change after observations:

Please attach updated documentation.