# 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 Library's POS (Point of Sale) 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 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.
**Firewall Access Rules**: Control a network device's ability to send traffic to, or receive traffic from, programs, system services, computers, or users.
**DSS**: Acronym for "Data Security Standard" and also referred to as "PCI DSS."
**Information Security**: Protection of information to insure confidentiality, integrity, and availability.
**Network Segregation**: Developing and enforcing a ruleset controlling which computing devices are permitted to communicate with which other 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 and
**PCI**: Acronym for "Payment Card Industry."
**POS**: Acronym for "Point of Sale."

### Guidelines
a. This policy applies to all Library employees and to contractors and consultants who have access to the cardholder data environment.
b. All employees who have access to cardholder data must attend security awareness training and acknowledge in writing that they have read and understand the Library's Information Security Policy. This policy will be reviewed with applicable staff annually.
c. The Library 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. The Library shall not accept payments via telephone.
e. No cardholder data shall be entered or stored in any computer system of the Library or in any electronic format of any kind.
f. Cardholder data may not be transmitted via email.
g. No more than the last four digits of a PAN shall be printed on either the Library copy or the customer copy of any receipts or reports.

## Responsibility

The Library trains staff on its Data 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. The Library shall not share personal 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 must be controlled. Receipts and reports containing cardholder data must always be kept in a secure area at the Patron Services Desk until they are delivered to the Office Manager.
d. No Library employee may divulge, copy, release, sell, loan, review, alter or destroy any information except as properly authorized.
e. Each employee must take appropriate measures to protect confidential information wherever it is located, e.g., held on physical documents, communicated over voice or data networks, exchanged in conversation, etc.

## Records

a. The Library shall retain 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 by a third-party service.

## Service Providers

The Library maintains and implements procedures to manage service providers with whom cardholder data is shared. The Library:

a. Maintains a list of service providers.
b. Maintains a written agreement with service providers. This agreement includes acknowledgement that the service providers are responsible for the security of cardholder data that the service providers 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

| FREQUENCY | DESCRIPTION |
|---|---|
| As Needed | • Track and monitor vendor access to Library systems. |
| Monthly | • Review firewall reports to verify any unauthorized access has been halted, or obtain documentation from the vendor that the Library's ports are being monitored. |
| Quarterly | • Use auditing and monitoring tools to verify that:<br>  ○ All prohibited inbound and outbound traffic is denied.<br>  ○ All router configuration files are secure and synchronized.<br>• Verify that perimeter firewalls between all wireless networks are configured correctly.<br>• Use a wireless analyzer to establish the validity of each wireless network that appears on the analyzer.<br>• Verify all daily operations are being performed. Verification that the tracking mechanism has successfully recorded completion of all tasks will be verified for a sample of days. |
| 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 updated as needed.<br>• Review relevant contracts to confirm that service providers acknowledge responsibility for protecting cardholder data. |

**References**
https://www.pcisecuritystandards.org/documents/SAQ_B-IP_v3.pdf

Hinsdale Public Library Board of Trustees
Approved and Adopted by Library Board on 08/28/2012.
Rev 01/26/2016.

**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 the Library plugged into the Library's network. The incident should be immediately reported to the IT Manager and/or LIC.

1) Staff Member's Name
2) Staff Member's Department
3) Date of Discovery
4) Time of Discovery
5) Location where the equipment was found
6) As detailed a description as possible
7) Fill out the owner's information, if known
8) If applicable, identify where the equipment was plugged into one of the Library's data wall/floor jacks
9) Include all known system information
10) Describe the physical security of the location where the equipment was found. Example 1: Teen Lounge – no physical security. Example 2: Server Room – Locked door, only accessible with inside key

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

# Rogue Wireless Access Point & Network Security Incident Form

**Staff Information:**

1. Name:_____
2. Department:_____
3. Date:_____
4. Time:_____

**5. Location(s) of rogue wireless access points/systems/devices:**

_____

_____

**6. Describe wireless access point(s)/system(s)/device(s) – 1 form per piece of equipment:**

Hardware Manufacturer:_____
Serial Number:_____
Corporate Property Number (or any other identifying ID tags):

_____

**7. Owner of the described equipment:**

Name:_____
Address:_____
Phone:_____

8. Is the affected system connected to the network? ☐ YES ☐ NO

9. System Name: _____
System Network Address: _____
MAC Address: _____

10. Describe the physical security of the location of affected information systems (locks, security alarms, building access….):

_____

_____

_____

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