Iowa City 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) terminals and through its website. 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.

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

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

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
- This policy applies to all Library employees and to contractors and consultants who have access to the cardholder data environment.
- All employees who have access to cardholder data must attend annual security awareness training during which this policy will be reviewed and are trained to be aware of suspicious behavior and to report tampering or substitution of devices
- 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 segmentation.
- The Library shall not accept payments via telephone.
- No cardholder data shall be entered or stored in any computer system of the Library or in any electronic format of any kind.
- Cardholder data may not be transmitted via email or other end-user messaging technologies.
- 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.
- The Library shall not share personal cardholder information with other companies or third parties.
- 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.

- 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 Help Desk until they are delivered to the Business Office.
- No Library employee may divulge, copy, release, sell, loan, review, alter or destroy any information except as properly authorized.
- 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.
- Staff are trained to report any incident that could affect cardholder data. An incident response plan is in place.

Records

- The Library shall retain receipts and reports containing cardholder data in a secure location until they are eligible for disposal.
- The library shall maintain a current list of POS devices which includes make, model, and serial number.
- The library maintains a schedule that outlines the frequency of required tasks for PCI compliance.

Service Providers

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

- Maintains a list of service providers.
- 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.
- Establishes a service provider's ability to meet these criteria before entering into an agreement with them.
- Monitors service providers' PCI DSS compliance status at least annually.
- Maintains information about which PCI DSS requirements are managed by each service provider.