Joseph P. Simpson Public Library
PCI - DSS (Payment Card Industry Data Security Standard) Policy
Approved November 11, 2014
Reviewed April 11, 2017

The standards are designed to protect cardholder information of patrons that utilize a credit card to transact business with the Library. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.

The Library must adhere to following requirements:

1. Build and maintain a secure network
2. Implement strong access control measures
3. Regularly monitor and test networks
4. Maintain an information security policy
5. Insure third party compliance
6. Provide staff training

General Requirements

- Management and staff who handle credit cards must be familiar and adhere to the PCI-DSS requirements of the PCI Security Standards Council.
- Executive Director must conduct an annual self-assessment against the requirements and report results to the Board of Trustees.
- All employees that are involved in the processing of credit card payments must sign a statement that they have read, understood and agree to adhere to the Information Security policies of the Library as well as this policy.
- Any proposal for a new process related to the storage, transmission or processing of credit card data must be brought to the attention of the Director.

Storage and Disposal

- Customer credit card information must not be entered or stored on the Library network server, workstations or laptops, or on any device that has an identifiable IP address (e.g. smart phone).
- If applicable, web payments must be processed using a PCI-compliant service provider approved by the Director. Credit card numbers must not be entered on a webpage of server hosted by the Library network.
- Any paper documentation containing credit card information should be limited to only information required to transact business and by only individuals who need to have access. It must be kept in a secure location.
- All credit card processing machines must be programmed to printout only the last four or first six characters of a credit card number.
- Sensitive cardholder data must be securely disposed of when no longer needed for reconciliation, business or legal purposes. In no instance shall this exceed four years. Secured destruction must be via shredding or a third party provider with a certificate of disposal.

Third Party Vendors

- The Executive Director, with the guidance of the Finance Committee, will approve all merchant banks or third party vendors that the library employs in the processing, storage and / or transmission of credit card data, regardless of the manner or duration of such activities.
- To the satisfaction of the Director and Finance Committee, all third parties involved in credit card transactions shall verify that they meet PCI security standards. Initial proof of compliance should be provided and the Executive Director, when completing self-assessment for PCI, should verify continued compliance.

Self-Assessment

- Self-Assessment will be performed annually by Library staff.
- The Library will complete the PCI-DSS Self-Assessment Questionnaire annually AND at any time a credit card related system or process changes. The assessment is the responsibility of the Director.
- The library staff will remediate any issues found during the assessment as a high priority work task.