PCI COMPLIANCE POLICY

~~November 8, 2021~~December 11, 2023

This policy outlines the library's compliance with the Payment Card Industry (PCI) Data Security Standards (DSS) that will be enforced on the library's premises.

PCI-DSS are network security and business practice guidelines adopted to establish a minimum-security standard to protect customer's payment card information. It is required for all merchants that store, transmit, or process payment card information. PCI-DSS is enforced by the credit card industry to help ensure payment data is protected from theft and fraud.

~~The Assistant Director will review this policy annually in accordance with the PCI Compliance Supplemental Checklist.~~

Protect Cardholder Data
Library users' credit card payment information will not be stored, transmitted or otherwise captured outside of the PCI Compliance Training Procedure. Any account numbers displayed on devices or receipts will be masked so as to not display more than four characters. (PCI Requirement 3.2, 3.3)

Encrypt Transmission of Cardholder Data
Credit card numbers are only to be transmitted by approved PIN Transaction Security (PTS) device in an encrypted state. Unprotected primary account numbers (PANs) will not be sent via end-user messaging technologies (such as e-mail or text messaging). A PAN is a unique payment card number, typically for credit or debit cards, that identifies the issuer and the particular cardholder account. (PCI Requirement 4.2)

Restrict Access to Cardholder Data
Access to the library's cardholder system is limited to only those individuals whose jobs require such access and who are appropriately trained. Privileges must be assigned to individuals based on job classification and function. (PCI Requirement 7.1) A PCI Compliance Incident Response procedure has been created in the event of a security breach.

Restrict Physical Access to Cardholder Data
Hard copies containing confidential or sensitive information (i.e. paper receipts, paper reports) will not be generated or stored. (PCI Requirement 9.5 – 9.8)

The Business Office has compiled and maintains a PCI Compliance List of Devices; the list includes make, model, serial number and location of device. Business Office staff will update this list as needed. Business Office staff are required to be trained and to conduct periodic inspections in accordance with the PCI Compliance Training Procedure, to detect suspicious behavior such as tampering or substitution of credit card devices. (PCI Requirement 9.9)

Personnel and Vendors
All library staff, with the exception of facilities staff, part-time non-benefited staff, and the director have approval to use listed devices. Refer to the City of Rapid City's Technology Resource Usage Policy for the following: Acceptable uses of the technologies. (PCI Requirement 12.1 – 12.6) The Business Office will also maintain a list of service providers, to include the contract and vendor's PCI Compliance certification. (PCI Requirement 12.8)

Annual Review

The Assistant Director will review this policy and all associated procedures annually based on the most up to date version of PCI DSS~~compliance~~ available~~-~~.

~~The Assistant Director will complete a PCI-DSS Self-Assessment Questionnaire B (version 3.2) annually.~~ The following documentation assists with the annual ~~compliance assessment~~review:

- PCI Compliance List of Devices
- PCI Compliance Incident Response Procedure
- PCI Compliance Training (Staff list)
- ~~PCI Compliance Supplemental Checklist~~PCI Compliance Quick Reference Guide (https://www.pcisecuritystandards.org)
- ~~PCI Compliance Training (Staff list)~~
- PCI-DSS (Payment Card Industry – Data Security Standards (https://www.pcisecuritystandards.org)

Revised December 11, 2023; November 8, 2021; October 14, 2019; created October 10, 2016