PCI COMPLIANCE POLICY

October 10, 2016

The purpose of this policy is to inform patrons and staff of the Rapid City Public Library of the Payment Card Industry (PCI) Data Security Standards (DSS) that the Library is expected to be compliant with and 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 a requirement for all merchants that store, transmit, or process payment card information. The PCI-DSS is enforced by the credit card industry and helps ensure payment data is protected from theft and fraud.

Protect Cardholder Data
Patron's credit card payment information will not be stored, transmitted or otherwise captured outside of the PCI Compliance Training Procedure. Any account #'s displayed on devices or receipts are to be masked so as not to 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) are not to 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 Rapid City Public Library's cardholder system components is limited to only those individuals whose jobs require such access and are appropriately trained. Privileges must be assigned to individuals based on job classification and function. (PCI Requirement 7.1)

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

A PCI Compliance List of Devices has been established; the list includes make, model, serial # and location of device. This list will be maintained as needed. Personnel are required to be trained and periodic inspections will be conducted, 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)

Information Security for Personnel
This policy will be reviewed in accordance with the PCI Compliance Supplemental Checklist on an annual basis. A list of all such devices has been established as the PCI Compliance Device Inventory; listed personnel has been established within the PCI Compliance Training Procedure. These personnel 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)

A list of service providers will be maintained to include the contract and vendor's PCI Compliance certification. (PCI Requirement 12.8)

An incident response plan (PCI Compliance Incident Response Procedure) has been created in the event of a security breach. All authorized personnel will be trained in accordance with the PCI Compliance Training Procedure. (PCI Requirement 12.10)

A PCI-DSS Self-Assessment Questionnaire B (version 3.2) is to be completed annually by the Rapid City Public Library. The following documentation assists with the annual compliance assessment:

- PCI Compliance Device Inventory
- PCI Compliance Incident Response Procedure
- PCI Compliance List of Authorized Personnel Users
- PCI Compliance Supplemental Checklist
- PCI Compliance Training Procedure

Created October 10, 2016