Reviewed and approved by Board - February 20, 2014
Revised by attorney; approved by Board - September 21, 2023

Payment Card Industry (PCI) Information Security Policy

Introduction

The purpose of this document is to educate all entities in the Joliet Public Library's payment environment and to explain and enforce the Joliet Public Library credit card security requirements by the Payment Card Industry Data Security Standard (PCI DSS) Program, which is a worldwide security standard assembled by the Payment Card Industry Security Standards Council. The PCI DSS requirements do not supersede local, state and federal laws and regulations.

The Joliet Public Library is committed to compliance with the PCI DSS to protect payment card data regardless of where that data is proposed or stored. This policy is to help assure that the Joliet Public Library is (1) being a good steward of personal information entrusted to it by its constituents, (2) protecting the privacy and cardholder data and information of patrons that utilize a credit card to transact business with the Joliet Public Library, (3) complying with the PCI DSS, and (4) striving to avoid a security breach from unauthorized and inappropriate use of cardholders' information.

Any failure to protect cardholder information may result in financial loss for the cardholder, suspension of credit card processing privileges, fines, and damages to the reputation of the Library. Questions regarding the policy should be directed to the Library Director. This policy shall be established, published, maintained and reviewed at least annually to reflect changes to business objectives and risk management.

To reduce the probability of a compromise of cardholder data at the Joliet Public Library, it is the Joliet Public Library's policy to not store cardholder information on Joliet Public Library systems.

E-commerce credit card transactions are outsourced. When an e-commerce customer is making a payment from the Joliet Public Library website, the payment page originates from an outsourcing vendor (ePay) and the payment data the patrons provide does not travel through any Joliet Public Library computer or network. The service is provided by the State Treasurer's Office.

The Joliet Public Library self-checkout units are handled through a third party vendor. The self-checkout units communicate through a payment gateway server using SSL encryption and a security certificate. The server then passes the transaction and it is handled through ePay, a service provided by the State Treasurer's Office.

To facilitate in-person transactions, the Joliet Public Library uses credit card terminals. All credit card terminal transactions communicate to a payment gateway server using SSL encryption and a security certificate. The server then passes the transaction and it is handled through a service provided by the State Treasurer's Office.

What is Payment Card Industry (PCI) Compliance?
The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding credit cardholder information for all credit card brands.

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The requirements apply to all methods of credit processing, from manual to computerized.

Scope of Compliance
The PCI requirements apply to all Joliet Public Library systems, employees or designated individuals and units that process, transmit or handle cardholder data in a physical or electronic format. Currently, Joliet Public Library cardholder environment consists only of standalone dial-out terminals and self-checkout stations. The environment does not include storage of cardholder data on any computer systems.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) B, ver. 2.0, October, 2010. Should Joliet Public Library implement additional acceptance channels, begin storing or otherwise become ineligible to validate compliance under SAQ B, it will be the responsibility of Joliet Public Library to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Any Joliet Public Library employee, contractor, consultant or agent who, in the course of doing business on behalf of the Library, is involved in the acceptance of credit card data, handles cardholder information, and/or is involved in the acceptance of electronic payments is subject to this policy.

Protecting Cardholder Data
1) Library users' credit card payment information will not be stored, transmitted or otherwise captured outside of these PCI compliance policies and procedures. Joliet Public Library will mask the display of PANs (primary account numbers) and limit viewing of PANs to only those employees and other parties with a legitimate need or whose jobs require such access and who are appropriately trained. The Joliet Public Library will only show the last four digits of the PAN on hard copy receipts of transactions.
2) Employees must be discreet and use common sense when handling cardholder data. Credit card numbers must not be transmitted in an insecure manner or via end user messaging technologies, such as by email, text messages, IM's, unsecured or stored fax or through interoffice mail. When physically transporting credit card data across the Joliet Public Library system, the information should be placed in an envelope marked, "Confidential" and sent by a delivery method that can be accurately tracked and trusted. Logs must be maintained to track all media that is moved from a secured area and management approval must be obtained prior to moving the media.
3) It is prohibited to store sensitive cardholder data (i.e., full account number, expiration date, PIN, card validation value, expiration date and service code CVV) in any Library system and/or department server, third-party software, personal laptop, flash drive, CD, cellular phones, personal digital assistants, portable electronic devices or on paper.
4) Employees shall not disclose or acquire any information concerning a cardholder's account without the cardholder's consent.

5) The entire credit card number must not be printed on either the merchant copy or customer copy or any receipts or reports.
6) All credit card receipts must be stored in a locked drawer or cash register at the Point of Sale station until they are placed in the safe at the end of the day.
7) All new employees who handle or have access to credit card data are required to attend in-house credit card security training prior to processing credit card payments. All employees who handle or have access to credit card data are required to attend in-house credit card security training annually. All employees who handle or have access to credit card data are also required to sign that they have read the Joliet Public Library Payment Credit Industry Security Policies and Procedures, the Point-of-Sale Credit Card Procedures and Security Training Information and have viewed the training video. A copy of the signed form will be given to the employee and a copy will also be placed in the employee's personnel file.

Maintain a Vulnerability Management Program
Joliet Public Library does not store cardholder data. However, some Joliet Public Library systems are used as virtual terminal devices for data entry of cardholder information. As such this section applies to the configuration of those workstations and affected servers.
1) Anti-virus software must be installed and remain current on all systems directly processing and/or transmitting credit card transactions.
2) Anti-virus software must be installed and remain current on all systems connected to systems that process and/or transmit credit card transactions.
3) Assure that changes to firewall hardware or software or security rules are based on industry best practices, all of which shall be in accordance with PCI DSS requirements.

Implement Strong Access Control Measures
1) All documentation containing card account numbers must be stored in a secure environment until processed. Secure environments include locked drawers, locked cabinets or safes with limited access to only individuals who are processing the credit card transaction.
2) Processing of credit cards should be done as soon as possible by a dedicated employee. Card expiration dates and card validation values from the back of cards must be masked.
3) All media used for credit cards must be destroyed when it is no longer needed for business or legal reasons. All hardcopy must be kept in a secure environment until they can be shredded with a cross-cut shredder prior to disposal. Secure environments include locked drawers, locked cabinets or safes with limited access to those individuals whose jobs require specific access.
4) Background checks must be performed prior to the hiring of any positions with access to cardholder information.
5) The Deputy Director or their designee will assign an individual to administer the control of log-in privileges, limit software access to secure locations and delete access to software for terminated employees and those employees whose responsibilities have changed. Access to system components and cardholder data must be limited to those individuals whose jobs require specific access.

Incident Reporting
1) An "incident" is a suspected or confirmed "data compromise." A "data compromise" is any situation where there has been unauthorized access to a system or network where prohibited, confidential or restricted data is collected, processed, stored or transmitted. A "data compromise" can also involve the suspected or confirmed loss or theft of any material or records that contain cardholder data. All incident detections and responses, especially related to critical systems, must follow this policy. Employees must be aware of their responsibilities in

detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

a) Theft, damage, or unauthorized access (i.e. unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).

b) Fraud – Inaccurate information within databases, logs, files or paper records.

c) Abnormal system behavior (i.e. unscheduled system reboot, unexpected messages, abnormal errors in system log files or on terminals).

d) Security event notifications (i.e. file integrity alerts, intrusion detection alarms and physical security alarms.

2) The Director or Deputy Director must be notified immediately of any suspected or real security incidents involving Joliet Public Library computing assets, particularly any critical system or system that handles or processes cardholder or other Personally Identifiable Information.

3) If it is unclear as to whether a situation should be considered a security incident, the Director or Deputy Director will be notified to evaluate the situation.

4) During off business hours, the Person-in-Charge will be notified of any possible security incidents. The Person-in-Charge will contact the Director or Deputy Director for further instructions.

5) If the incident involves a compromised computer system, the following steps will be taken:

a. Do not alter the state of the computer system. The computer system should remain on and all currently running computer programs left as is. Do not shut down the computer or restart the computer or change passwords.

b. Do not switch off the compromised machine; instead, isolate the compromised system(s) from the network by immediately disconnecting the computer from the network by removing the network connection cable from the back of the computer.

c. Report the security incident to the Director or Deputy Director. The Director or Deputy Director will contact the Manager, End User Technologies to report any suspected or actual incidents and gain assistance in determining further action.

d. No communications should occur with anyone outside of the immediate supervisor and authorized individuals. All communications with law enforcement or the public will be coordinated by the Director or Deputy Director.

e. Any known information should be documented while waiting for the Director or Deputy Director and the Manager, End User Technologies to respond to the incident. If known, include the date, time, location and nature of the incident, all personnel involved, any action taken, the person performing the action, and the person performing documentation.

Incident Severity Classification

The Director, Deputy Director, and Manager will first attempt to determine if the security incident justifies a formal incident response.

In cases where a security incident does not require an incident response, the situation will be forwarded to the technology support team to ensure that all technology support services required are rendered. The following descriptions should be used to determine what response the technology support team should take:

1) **Level 1** – One instance of potentially unfriendly activity (i.e., port scan, corrected virus detection, unexpected performance peak, etc.)

2) **Level 2** – One instance of a clear attempt to obtain unauthorized information or access (i.e. attempted download of secure password files, attempt to access restricted areas, single

computer successful virus infection on a non-critical system, unauthorized vulnerability scan, etc.) or a second Level 1 attack.
3) **Level 3** – Serious attempt or actual breach of security (i.e. multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful buffer/stack overflow, successful unauthorized access to sensitive or critical data or systems, broken lock, stolen papers, etc.) or a second Level 2 attack.

Incident Response Plan and Procedures
Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls. The following actions should be taken by the Director, Deputy Director and/or Manager, End User Technologies and the technology support team once an incident has been identified and classified.

1) **Level 1 – Contain and Monitor**
a. If possible, record the user, IP address and domain of intruder.
b. Utilize approved technology controls to temporarily or permanently block the intruder's access.
c. Maintain vigilance for future break-in attempts from this user or IP address.

2) **Level 2 – Contain, Monitor and Warn**
a. Collect and protect information associated with the intrusion.
b. Utilize approved technology controls to temporarily or permanently block the intruder's access.
c. Research the origin of the connection.
d. Research potential risks related to intrusion method attempted and re-evaluated for higher classification and incident containment, eradication, and recovery as described for Level 3 incident classifications.

3) Level 3 – Contain, Eradicate, Recover and perform Root Cause Analysis
a. If the incident involved credit card systems the acquirer and applicable card associations must be notified.
b. Contain the intrusion and decide what action to take. Consider unplugging the network cables, applying highly restrictive ACLs, deactivating or isolating the switch port, deactivating the user ID, terminating the user's session/change password, etc.
c. Collect and protect information associated with the intrusion via offline methods. In the event that forensic investigation is required the technology team will work with legal and management to identify appropriate forensic specialists.
d. Eliminate the intruder's means of access and any related vulnerabilities.
e. Research the origin of the connection.
f. Research potential risks related to or damage caused by instruction method used.

Credit Card Compromise – Special Response
For any incidents involving potential compromises of credit card information, the technology team will use the following procedure:
1) Contain and limit the exposure. Conduct a thorough investigation of the suspected or confirmed loss or theft of account information. To facilitate the investigation:
a. Log all actions taken.
b. Utilize chain of custody techniques during all transfers of information related to the incident.

c. Do not access or alter compromised systems (i.e. do not log on or change passwords; do not log in as ROOT).
d. Do not turn off the compromised machine. Instead, isolate compromised systems from the network by unplugging the network cable. To preserve the evidence for a forensic investigation, it is extremely important to not access the system.
e. Preserve logs and electronic evidence. Be on high alert and monitor all cardholder information systems.
2) Notify the following:
a. Merchant bank
b. Local FBI Office
c. U.S. Secret Service (if Visa payment data is compromised)
d. Local authorities if applicable
3) Follow appropriate procedures for each association which Joliet Public Library utilizes for credit card services per below:

- **Visa**

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

- **MasterCard**

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

- **Discover Card**

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.
4) Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm
5) Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Manager, End-User Technologies will work with legal and management to identify appropriate forensic specialists.
6) Eliminate the intruder's means of access and any related vulnerabilities.
7) Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned
Not more than one week following the incident, members of all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly. Upon conclusion of the investigation, systems will be restored to their non-compromised state.