307 / Administration

Credit Card Security

The Villa Park Public Library is committed to following the requirements of the Payment Card Industry Data Security Standard (PCI DSS) program in order to protect and secure all credit card transactions which are processed at the library in the course of conducting library business. The library has instituted departmental procedures for safeguarding cardholder information and securing the storage of data. This pertains to all transactions regardless of how they are initiated.

This policy shall be reviewed annually and updated as needed to reflect changes to business objectives or the risk environment.

Scope

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, the Villa Park Public Library cardholder environment consists only of imprint machines or stand-alone dial-out terminals. The environment does not include storage of cardholder data on any computer system. If, in the future, the library implements additional acceptance channels or begins to store, process, or transmit cardholder data in electronic format, the library will determine and implement the appropriate policies and controls, as required for PCI compliance.

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

Protection of Credit Card Data

All employees are required to adhere to the policies and procedures designed to secure credit card data. Employees shall not use vendor-supplied defaults for system passwords. Group, shared, or generic accounts and passwords are prohibited. Employees who handle or have access to credit card data must complete PCI security training prior to working with PCI data and systems.

Internal or external distribution of any kind of media containing cardholder data is prohibited. Credit card numbers must not be transmitted in an insecure manner, such as by email, IM's, unsecured or stored fax, or through mail. Printing and scanning cardholder information is not permitted.

Anti-virus software must be installed and remain current on all systems directly processing and/or transmitting credit card transactions. Anti-virus software must be installed and remain current on all systems connected to systems that process and/or transmit credit card transactions.

The library has instituted processes to ensure credit card data is not stored and data is deleted post-authorization so that the data is unrecoverable.

- The full contents of any track data from the credit card are not stored under any circumstance. This includes data contained on the magnetic strip located on the back of a credit card or equivalent data contained on a chip on a credit card.
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance.
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance.

The library has instituted procedures to secure PANs (primary account numbers).

- The display of PANs is masked. A properly masked number will show no more than the first six and the last four digits of the PAN.
- The viewing of PANs is limited to only those employees and other parties with a legitimate need.
- Sending unencrypted PANs by end-user messaging technologies is prohibited.

Physical access to cardholder data and all confidential or sensitive information is restricted. All cardholder data, whether hard copy or electronic, are physically secured. Access to these data is limited to only those employees whose job functions require such access. These data are locked. Strict control is maintained over data storage and access to these data.

All media containing cardholder data is destroyed when no longer needed for business purposes or legal reasons. All hardcopy must be shredded with a cross-cut shredder prior to disposal.

Protection of Payment Devices

The library is committed to protecting all payment devices that capture credit card data by physical interactions with a credit card are protected from tampering or substitution. Payment devices are checked periodically to ensure that no tampering or substitution has occurred. Library staff who interact with payment devices are provided with training necessary to identify if a payment device has been compromised by tampering or substitution.

The library maintains a current list of devices, including make and model, location, and serial number, of each payment device.

Service Provider Requirements and Approval

Service providers must receive approval from the Library Director or the Director's designee to process credit card payments and/or before entering into any contracts or purchases of software and/or equipment related to credit card processing. Due diligence prior to engaging a service provider will be done to monitor their PCI DSS compliance status and how compliance is managed.

Written agreements with each service provider shall include an acknowledgement that the service providers are responsible for the security of the cardholder data to which they have access.

All third parties with access to cardholder data are contractually required to adhere to PCI DSS requirements and provide proof of PCI certification to the merchant department. Written agreements must include the service provider's statement of responsibility regarding the security of cardholder data that is processed, transmitted, and/or stored on its system.

Ecommerce merchants must provide the library with all public IP addresses used in the processing and/or transmitting of credit card data for the purpose of performing required external scans.

Ecommerce merchants who input card information directly into their payment application, for example, mail orders and/or telephone orders, are required to use secure PC's designated for that single purpose.

Merchants must notify the library of system changes, software upgrades and personnel changes related to credit card processing.

Reporting and Handling an Incident

The Library Director and the Department Head should be notified immediately of any suspected or real security incidents involving cardholder data to ensure timely and effective handling of all incidents.

The notifying employee should not communicate details or generalities about the suspected or actual incidents with any other employees. The employee should document any information about the incident, including date, time, and nature of the incident.

The response to a suspected or actual incident will follow these steps:

- Identification and information collection about the incident
- Severity classification of the incident
- Containment, eradication, recovery, and root cause analysis of the incident

Steps to be taken

- Notify applicable card associations
- Alert all necessary parties, including merchant bank, local authorities, local FBI office, and the U.S. Secret Service if Visa payment data is compromised
- Collect and protect information associated with the incident
- Eliminate the means of access and the vulnerabilities
- Research potential risks related to or damage caused by the intrusion method used

Within one week of the incident, the Library Director, Deputy Director, Automation Services Coordinator, and all affected parties will meet to discuss the results of any investigation to determine the cause of the incident and to review security controls to determine their appropriateness for current risks. Any identified areas in which the response plan, policy or security control can be made more effective or efficient must be addressed accordingly.

Approved 06/22/2022