Credit Card Security

Created 16 Apr 2014
Revised 16 Apr 2014
Reviewed 16 Apr 2014

Purpose

This policy is intended to ensure customer personal information, particularly credit card information and primary account numbers are securely stored. The Library will strive to maintain the highest level of reasonable security for all patron and credit card information that is gathered or used in the course of its operations.

Scope and Responsibility

This policy applies only to a payment application accessed remotely through the Library's website or to point-of-sale software accessed through the Library's staff workstations via IP based stand-alone credit card terminals to a vendor that processes and stores credit card data and cardholder information.

The Library employs personnel to ensure the safe and secure operation of its network to the best of their knowledge and ability, utilizing general accepted business practices and experienced judgment.

For all hardware and software used by the Library, necessary passwords shall be changed from the original vendor default password to a strong password, maintained by the Library in accordance with generally accepted business practices.

Electronic Data Security: Security Codes

Under no circumstances shall the security code, which is sometimes called the CVV or CVC value, be stored on any Library equipment nor by its credit card processing vendor. (This number is found printed on the signature block of the card on MasterCard, Visa and Discover and printed on the front of American Express cards.)

Employees may collect this value directly from a card or verbally from the cardholder over the phone. It may be entered into a terminal or computer where it is erased after authorization.

The PIN number on debit/ATM cards is not stored locally on any of the Library's equipment.

If sensitive authentication is received, it shall be immediately deleted and processes shall be in place to securely delete the data and verify that it is unrecoverable by the software vendor.

Electronic Data Security: Cardholder information

Cardholder data is not stored on any of the Library's computer equipment. This means no storage on workstations, laptops or personal computers is permitted, even for brief periods of time.

Under no circumstances are the full contents of the magnetic stripe to be recorded or stored in any fashion on any of the Library's equipment. Cardholder information is encrypted or truncated to the last four digits at all times when stored. When data is displayed in reports or on user screens the Cardholder numbers shall be masked so that a maximum of the last four (4) digits of the number are printed of displayed.

When credit card data is sent over public networks, such as the Internet, it must be encrypted (encryption is provided by the Library's credit card processing vendor). Access control to cardholder information records shall be on a strict need-to-know basis only. All other traffic is to be denied unless specifically authorized.

The Library does not use modems to transmit any credit card information.

The Library's wireless networks are secured in accordance with currently accepted business practices. The Library's staff do not use wireless network to transmit patron or credit cardholder information.

The Library does not create, as a usual business practice, any paper records of credit card account numbers (cardholder information). Whenever such information is obtained or gathered, the records will be stored in a locked/secure area until destroyed. Paper records of cardholder information and data shall not be left unattended when in use. Employees who must leave the work area while cardholder information records are outside of the locked file shall secure them in a drawer, a locked room or return them to the file.

If Cardholder information is part of a data entry or order form they must be destroyed by shredding after data entry and verification.

The Library does not collect cardholder information by fax as a part of its regular business. If such information is sent via fax, the fax machine shall be secured or attended while receiving cardholder information. Faxes shall be treated the same as paper records.

Record and Data Backup Retention and Destruction

Credit card information and records will be retained for no more than 2 years. Credit card information is not retained on the Library's equipment and should be destroyed immediately after the transaction

is completed unless they are the only transaction record. In that case, they must be retained for 2 years. The cardholder information may be obliterated leaving no more than the last 4 digits of the card number to increase security.

The Library does not retain any long term records of credit card information for its patrons.

Destruction of credit card information shall be performed securely by either an employee or a secure destruction service must be through shredding, incinerating or pulping. In the case of electronic media "degaussing" may be used.

Each employee who handles or uses credit card information or cardholder information data shall be screened appropriately (background check) before being granted access to this data.

The Library does not, as a regular course of business, solicit or send credit card information via email, instant messaging or chat. If such information is sent or received, the Library will ensure that the information is encrypted using proven, standard algorithms.

The Library will act to ensure security on all of its equipment. Only necessary services, protocols, daemons, etc. directly necessary for the function of the Library's systems may be enabled. All unnecessary services, protocols, daemons, etc. shall be disabled.

Encryption

Software applications used by the Library or its vendors must use strong encryption. Symmetric cryptosystem key lengths must be at least 128 bits. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Library's management. Encryption keys shall be split between two individuals and stored under lock and key. No single individual is allowed to manually decrypt sensitive files without the knowledge of the other authorized individual.

Cardholder information and data is to be encrypted at all times when stored. When data is displayed in reports or on user screens the card number shall be masked so that only the last four (4) digits of the number are printed of displayed. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Keys must be changed as deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically at least annually. Old keys must be destroyed. Unauthorized substitution of keys is prohibited. Known or suspected compromised keys must be replaced upon discovery. Old or invalid keys must be revoked. Key custodians must sign for responsibility and acknowledge that they understand and accept their key-custodian responsibilities.

Non-Console Administrative Access

All non-console or web based administrative access, if applicable, shall be encrypted using technologies such as SSH, VPN, SSL/TLS as follows:

- Access shall be encrypted with strong cryptography and a strong encryption method before an administrative password is requested.
- System services and parameter files shall prevent the use of Telnet and other insecure login commands.
- Administrator access to web based management interfaces shall be encrypted with strong cryptography.

Cardholder data transmitted across open public networks
This section generally refers to the Library's Internet browser, such as; Internet Explorer, FireFox, Safari, Chrome, etc. The Library will ensure that all browsers used on its equipment meet these requirements:

The latest version of the browser is installed and it is set to automatically update.
Security settings are implemented by the Library's IT staff. SSL 3 and TTLS 1 are enabled on all browsers and verified.

Strong cryptography and security protocols, such as SSL/TLS, SSH or IPSEC, shall be used to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS include but are not limited to the Internet and wireless technologies.

Only trusted keys and/or certificates shall be accepted.

Security protocols shall be implemented to use only secure configurations, and not support insecure versions or configurations. Proper encryption strength shall be implemented for the encryption methodology in use by the vendor.

The Library will ensure that "HTTPS" appears as part of the browser Universal Record Locator (URL). Cardholder data shall only be required when HTTPS appears in the URL.

Industry best practices (for example, IEEE 802.11i) shall used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. (The use of WEP as a security control was prohibited as of 30 June, 2010.) PANs shall be rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, or chat).

Anti-virus
Anti-virus software is installed on all Library equipment. Administrative default accounts and passwords shall be changed regularly as part of the Library's general operations according to standard business practices for administrative user names and passwords.

Anti-virus software capable of detecting, removing and protecting against all known types of malicious software shall be deployed on all systems that are vulnerable. The anti-virus software shall

be set to automatically update. This feature is to be set so the user cannot bypass the updates. Regardless of automated updates personnel shall ensure that anti-virus definitions are up to date. Automatic scanning shall be enabled. Anti-virus software shall generate audit logs and maintain those records to the limit of the software employed.

Vendors

The Library does not retain any credit card information on its own as a part of its regular operations. For cardholder information shared with vendors the following controls shall be in place:

- Written acknowledgment by the vendor they are responsible for credit card information in their possession.
- Prior to engaging the vendor due diligence shall be performed.
- Evidence of PCI compliance shall be obtained annually.

Definitions

Credit Card Information – This is made up of 4 elements, the Primary Account Number (PAN), Cardholder Name, Service Code and Expiration Date. When these elements are found in association with each other they must be protected.

PAN– cardholder name, card number and expiration date. The cardholder information is always protected, either by encryption, masking or if stored on paper, placing in secure storage.

Encryption Algorithm – A method of scrambling or encoding data so that it cannot be read by unauthorized persons. Encryption algorithms usually start with large prime numbers and perform calculations to yield large numbers of variable length, complex "keys" that are difficult or impossible to decode by individuals or computers.

Encryption – A method of sending messages and information over an insecure channel, such as the Internet. Also used to prevent unauthorized persons from viewing or using data stored electronically.

Proprietary Encryption - An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem - A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem - A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).