Income and Disbursements Policies

"Connecting you to big ideas wherever you are!"

Deposits

Created 19 Jul 2000
Revised 19 Apr 2011
Reviewed 16 Nov 2016

Cash deposits for fine and fees

In order to provide segregation of duties in the accounting function, cash income from the Library's operations (fines, fees, and similar payments) are handled at each branch by the Branch Manager (or designee).

Other circulation staff may also be involved in the actual counting of "day end" receipts. The Branch Manager is responsible for ensuring that the daily receipts match the records that are provided in the Library's automation system. Any discrepancies are noted on the Library's *Record of Deposit* form.

Deposits are made weekly. A record of deposits is sent to the Business Office.

Credit card deposits for fines and fees

Credit card payments are made from the Library's public service desks using staff computers or through the Internet directly by the Library's patrons. In either case, payments are processed through the Library's automation system to a third party vendor and then deposited directly into the Library's banking account less any processing fees that have been incurred.

Payments made by credit card are recorded by the Library's staff as a part of their weekly reconciliation of funds received for fines and fees. The Library Accountant reviews reports of deposits made directly to the Library's banking accounts through credit card payments. These reports are reconciled to the reports created at the branch level.

Other deposits

All other cash and checks (taxes, grants, donations, and other similar income) are recorded by the Library Director or designee (other than the Library Accountant) in a log listing:

- Date received;
- Payer;
- Type of Income;
- Amount;
- Date of deposit.

A deposit slip is prepared by the Library Accountant and appropriate copies for documentation are made.

The Library Director (or designee) reviews and initials deposit slip indicating that the deposit totals agree with the log.

The Library Accountant (or designee) completes deposit transactions with the bank(s) and maintains records of those transactions.

Disbursements

Created 19 Jul 2000
Revised 19 Nov 2014
Reviewed 16 Nov 2016

Review of invoices

All invoices for supplies and library materials are reviewed, checked for accuracy, and approved by the department which placed the order. The invoices are compared with the order's documentation and packing slips to verify the material was ordered by the Library, received in good condition, and the charges are correct.

The Library Director or designee approves all invoices for payment.

The Library Accountant prepares checks for payment and records these transactions in the Library's accounting program.

Check signatories

Check signing ability is vested with the Library Board. The Library Board may designate check signing ability as necessary to its individual members or staff members. Generally, signers will include:

- President;
- Treasurer;
- Library Director;
- One other library manager.

(Due to the separation of duties, the ability to sign for payments may not be given to the Library Accountant.)

All payments are accompanied by an invoice or other documentation indicating the purpose of the payment and filed for audit. The Library Director or designee (other than the Library Accountant) checks that the charged amount equals the check amount and initials the documentation indicating it was reviewed.

A staff member is not authorized to sign checks in which s/he would be the recipient of the funds expended.

Refunds to patrons

Created 16 Apr 2014
Revised 19 Nov 2014
Reviewed 16 Nov 2016

When a patron erroneously makes payment (including credit card payments) to the Library for lost materials, staff are authorized to issue a refund in amounts less than $50 in cash.

When a refund is required that exceeds $50, a *Refund Authorization for Returned Material* form is sent to the Business Office and a check is issued and mailed to the patron. A copy of this refund form can be given to the patron if a receipt is needed.

If the payment was originally made by credit card, then a refund is credited to the patron's credit card by the Library Accountant. A *Refund Authorization for Returned Material form* must be completed for all credit card refunds and sent to the Business Office.

Charges for lost materials that are returned in the Library's outside item returns, or otherwise returned with the patron not present, will have the value credited to the patron account.

Credit Card Security

Created 16 Apr 2014
Revised 19 Nov 2014
Reviewed 16 Nov 2016

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 CSV 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.

Encryption 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 encryption 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 encryption 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 be 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 of the Library's 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).

Data breach

The Library does not store credit card information on its computer equipment. The Library uses encrypted methods for transmitting credit card transactions and use secure, segregated data networks for transmission of credit card data.

Personal information about patrons (such as name, address, date of birth, email addresses, and phone numbers) are stored locally. This information is stored electronically on the Library's server and is protected by the Library's network firewall. The firewall software and equipment are updated to remain current. The Library employs a dedicated information technology professional who

receives daily reports on the network and server operations including any anomalies that have been detected by the system.

In addition to these measures, the Library will periodically scan its network for unusual activity or connections. Unused data ports will be disabled as quickly as possible. The Library's staff network is limited to staff use only and any unauthorized access to that network is prohibited. The staff network is monitored for any unusual activity. The public network, including the pubic wireless access points, are monitored for unusual activity including attempts to gain admittance to the staff network.

Any suspected or actual data breach is reported to the Library Director immediately. The Library maintains procedures with its information technology officer and Public Relations Manager for response. The Library's insurance carrier (currently KACo) would also help the Library to coordinate a data breach response and to mitigate/assess damage.

Bank Statements and Reconciliation Reports

Created 19 Jul 2000
Revised 19 Apr 2011
Reviewed 16 Nov 2016

The Library Accountant compares bank statements monthly with interest earned, deposit records, and cancelled checks. A reconciliation report in the accounting program is prepared. The statement and reports are reviewed and approved by the Library Director (or designee).

The Board reviews and approves a monthly log of all account balances, a record of checks issued during the previous month, and a monthly update of income/expenditures as compared to the Library's annual budget.

Construction or Other Major Projects

Created 19 Jul 2000
Revised 15 Nov 2005
Reviewed 16 Nov 2016

Major projects may have a budget and bank account separate from the Library's general budget and bank account. Any separate budgets or bank accounts are subject to the same policies and procedures as the Library's general accounts.

Upon completion of the project, these accounts may be audited separately from the Library's annual audit as required.

Operations Income

Created 19 Jul 2000
Revised 21 May 2014
Reviewed 16 Nov 2016

Controls over monies received at each branch are implemented by the Branch Managers in regard to funds handled by the branch.

Fines and Fees

Documentation from the Library's automation system is provided to the Business Office to verify receipts and deposits for all fines and fees collected by each branch. A receipt for all payments or waivers is always given to the patron.

Branch Cash Drawers

Each day the cash drawer at each branch begins with a standard amount of money:

- Cold Spring Branch: $100.00
- Carrico Branch: $100.00
- Newport Branch: $100.00

A separate "bank" amount of $92.00 is kept at the Newport Branch only for making change for larger bills.

Before opening for business each day, the money in the cash drawer is counted and restored to the standard amount. All excess cash is recorded and added to the Bank. Any significant shortages are noted and investigated as needed.

After each weekly reporting period, the Bank is restored to the original amount. The cash form for money received is balanced against the cash in excess of the original amount from the Bank. The cash is prepared for bank deposit and deposit is made. Deposit slip receipt, cash form, and automation system financial reports documenting income are forwarded to the Library Accountant for review.

Waivers

A reason and adequate notes are required for every waiver of library fines or fees. All staff members are authorized to make waivers up to $10.00. Waivers over $10.00 are referred to a supervisor. The Director will investigate any suspected abuse of waivers by Library staff.

Staff Reimbursements for Purchases

Created 19 Jul 2000
Revised 14 Nov 2006
Reviewed 16 Nov 2016

Books and Other Items

Library staff, Board members, and Volunteers may purchase materials on accounts maintained by the Library. A log of materials ordered by staff is maintained by the librarian responsible for acquisitions. A different staff member records the receipt and payment for each item. The person who initiates the log preparation periodically reviews the log to insure that payments are being made within a reasonable time.

Staff Computer Purchases

With the approval of the Library Board, the Director may allow staff to purchase computers through the Library for their own personal use. Employees may be allowed to purchase the computers through a payment plan set up by the Director. Purchase and reimbursement of such purchase should occur during the same fiscal year. Purchases made on a payment plan must be reimbursed in total at the time of termination.

Review of Director's Expenses

Created 19 May 2009
Revised 19 May 2009
Reviewed 16 Nov 2016

The Board of Trustees is responsible for reviewing the expenses of the Library Director.

Expenses for the Director's salary and benefits are contractual. The contract is reviewed at the end of each contract term by the Board and the Director.

Expenses for the Director's travel on library business will be approved by the Board as a part of the regular budgeted annual expenses of the Library. The travel expenses for the Director will be budgeted separately and monitored separately from other line item expenses.

The Library-issued credit card for the Director is intended to be used in the conduct of the Library's business. The charges made upon the Director's Library-issued credit card are reviewed each month by the Treasurer.

All reimbursements and expenses for the Director are reviewed by the Library's independent auditor each year.

Petty Cash

Created 19 Jul 2000
Revised 14 Nov 2006
Reviewed 16 Nov 2016

The Petty Cash fund is to be used for small purchases or for purchases to solve an immediate need when a Library-issued credit card is not available or is not practical to use.

Each branch will maintain a Petty Cash fund of $100.00 in its safe. Only Branch Managers should access these funds. Transactions should be reimbursed only with a receipt. At any time total cash and receipts will equal $100.00.

When cash is low, the Branch Manager can request funds equal to the total amount of receipts to replenish the Petty Cash fund. The request is made by completing a Petty Cash Request form and submitting it with receipts to the Library Director or designee.

The Library Director or designee may conduct an unscheduled check of all Petty Cash funds to insure proper handling.

Library-Issued Credit Cards

Created 15 Jul 2003
Revised 19 Nov 2009
Reviewed 16 Nov 2016

Credit cards are issued to staff members who frequently make purchases for Library events, have frequent travel expenditures, or who order supplies and equipment for the Library.

The amount of available credit on each card is determined by the Library Director. The amounts of available credit on staff accounts are reviewed by the Library Accountant regularly.

Balances on credit cards are paid in full by the Business Office each month.

Staff members who use Library-issued credit cards maintain all receipts for expenditures. An individual statement is prepared for each credit card. The statement is sent to the staff member holding the card. The staff member checks all expenditures listed on the statement against his/her receipts. If the charges listed and receipts match, the statement is initialed and dated. The statement and receipts should then be sent to the Business Office for payment.

Charges on Library-issued credit cards are reviewed each month by the Director. The Director reviews the master list of credit card charges after the individual statements are reviewed/approved by the cardholder.

Charges on the Director's Library-issued credit card are reviewed by the Treasurer each month.

Fraud Prevention

Created 17 Nov 2009
Revised 17 Nov 2009
Reviewed 16 Nov 2016

Fraud is defined as a willful or deliberate act with the intention of obtaining an unauthorized benefit, such as money or property, by deception or other unethical means.

All fraudulent acts or related misconduct are included under this policy and include, but are not limited to, such activities as:

- Embezzlement, theft, misappropriation or other financial irregularities;
- Forgery or alteration of documents (checks, time sheets, contractor agreements, purchase orders, other financial documents, electronic files);
- Improprieties in the handling or reporting of financial transactions;
- Misappropriation of funds, securities, supplies, inventory or any other asset (such as furniture, fixtures, equipment, materials), including assets of the Library, patrons, suppliers, or others with whom there is a business relationship;
- Authorizing or receiving payment for goods not received or services not performed;
- Authorizing or receiving payments for hours not worked or expenses not accrued and documented;
- Profiteering as a result of insider knowledge of the Library's activities.

Fraud and related misconduct will not be tolerated. Employees found to have participated in such conduct will be subject to disciplinary action, up to and including termination.

Trustees and employees are expected to use their best efforts to recognize risks and exposures inherent to their areas of responsibility and to be aware of indications of fraud and related misconduct. Any Trustee or employee who knows or suspects fraud or related misconduct shall report that to the President of the Board of Trustees or the Library Director.

When fraud or related misconduct is reported, an appropriate investigation and all necessary action will be undertaken. All investigations of alleged wrongdoing will be conducted in accordance with applicable laws and Library policies/procedures. During or following the investigation, the Board may choose to consult with legal counsel and take appropriate steps to minimize recurrence.