Income and Disbursements Policies

"Connecting you to big ideas wherever you are!"

Deposits

Created 19 Jul 2000
Revised 18 Dec 2024
Reviewed 18 Dec 2024

Cash deposits for fees and charges

In order to provide segregation of duties in the accounting function, cash income from the library's operations (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 *Weekly Income and Deposit* form.

Deposits are made frequently. A record of deposits is sent to the library bookkeeper. The library bookkeeper uses the library's automation system and bank statements to reconcile cash income and deposits reported by the branches.

Credit card deposits for fees and charges

Credit card payments are made from the library's public service desks using secure internet devices provided by a third-party vendor. Payments are recorded in the library's automation system without any credit card information. Payments are deposited directly into the library's banking account less any processing fees that have been incurred.

The library bookkeeper compares records provided by branch staff against statements provided by the third-party vendor and the bank's record of deposits into the library's banking accounts.

Public copiers and printers

The library owns copiers and printers for the use of the public. The charges for the use of these machines is set by the board. Patrons may pay for these services in cash or by credit card.

Cash payments are collected by the branch managers on a monthly basis. Other staff members may occasionally collect cash payments. These payments are deposited by the branch managers and noted on the library's *Weekly Income and Deposit* form.

Credit card payments are processed through the vending devices for each machine by a third-party vendor. These payments are deposited directly into the library's accounts on a weekly basis by the vendor. The library bookkeeper reviews the statements and deposits to ensure accuracy.

When a patron uses a credit card, a temporary hold is placed on the patron's credit card for the full amount of possible charges (currently five dollars). This hold is released after the payment for the actual charges is processed. The hold is generally released within 48 hours.

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 bookkeeper) in a log listing:

- Date received
- Payer
- Type of Income
- Amount

A deposit slip is prepared by the library bookkeeper 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 bookkeeper (or designee) completes deposit transactions with the bank(s) and maintains records of those transactions.

Disbursements

Created 19 Jul 2000
Revised 15 Nov 2023
Reviewed 18 Dec 2024

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.

Invoices for services are approved by the department which authorized the service. Final invoices for services should not be authorized for payment until the entire project is satisfactorily completed. Partial payments for services based on the stages of the work to be completed should be clearly determined in contract or by written quote. No prepayment for services in excess of 50% of the quoted/contracted total cost will be paid and ideally will coincide with the projected cost of materials for the work to be performed.

The library director or designee approves all invoices for payment.

The library bookkeeper 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 manager from the library

Due to the separation of duties, the ability to sign for payments may not be given to the library bookkeeper. (Online payments still require two signatures before being authorized.)

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 bookkeeper) 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 the signer would also be the recipient of the funds expended.

Online bill payments

For security, where possible, all vendors are paid using online bill payment through the bank's website. Invoices paid online are treated as if it is being paid with a live check. A payment is not made online until two signatures authorize the payment. Online payments are processed through the library's regular banking accounts and are recorded in the library's accounting system. These payments, along with all other payments, are reported to the board each month as a part of the check register.

Refunds to patrons

Created 16 Apr 2014
Revised 15 Nov 2023
Reviewed 18 Dec 2024

Circulation fees and charges

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 library bookkeeper 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 branch staff or the library bookkeeper. A *Refund Authorization for Returned Material form* must be completed for all credit card refunds and sent to the library bookkeeper.

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.

Copier and printer charges

The library bookkeeper has the ability to refund erroneous charges to a patron for copies and prints. Staff members will inform the library bookkeeper of the date, time, location, and machine (copier or printer) where the charge was made along with the amount to be refunded.

Credit Card Security

Created 16 Apr 2014
Revised 18 Dec 2024
Reviewed 18 Dec 2024

Purpose

This policy outlines and explains Campbell County Public Library District's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program.

The Campbell County Public Library is committed to these security policies to protect information utilized by the library in attaining its business goals. All employees are required to adhere to the policies described within this document.

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Campbell County Public Library's cardholder environment consists only of limited payment applications (typically point-of- sale systems) connected to the Internet through its own LTE modem, but does not include storage of cardholder data on any computer system.

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) C, ver. 3.0, released February, 2014. Should Campbell County Public Library implement additional acceptance channels, add additional connected systems, begin storing cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of the Campbell County Public Library to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. Access to the Internet must be through a firewall, as must any direct connection to a vendor, processor, or service provider. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted by the firewalls to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment. (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized by management and controlled by the firewall. (PCI Requirement 1.3.5)
- Firewalls used to protect the cardholder data environment must implement stateful inspection, also known as dynamic packet filtering. (PCI Requirement 1.3.6)

Any mobile and/or employee-owned computers with direct connectivity the Internet (for example, laptops used by employees), which also have the ability to access the organization's cardholder data environment must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

Requirement 2: Do Not Use Vendor-supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor- defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to: (PCI Requirement 2.1.1)

- Default encryption keys
- Passwords
- SNMP community strings
- Default passwords/passphrases on access points

- Other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption (such as WPA or WPA2) for authentication and transmission of data over wireless networks.

Configuration Standards for Systems

Configuration standards for all system components must be developed and enforced. Campbell County Public Library must ensure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. (PCI Requirement 2.2)

Configuration standards must be updated as new vulnerability issues are identified, and they must be enforced on any new systems before they are added to the cardholder data environment. The standards must cover the following:

- Changing of all vendor-supplied defaults and elimination of unnecessary default accounts.
- Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (PCI Requirement 2.2.1)
- Enabling only necessary services, protocols, daemons, etc., as required for the function of the system. (PCI Requirement 2.2.2)
- Implementing additional security features for any required services, protocols or daemons that are considered to be insecure. (PCI Requirement 2.2.3)
- Configuring system security parameters to prevent misuse
- Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. (PCI Requirement 2.2.5)

System administrators and any other personnel that configure system components must be knowledgeable about common security parameter settings for those system components. They must also be responsible to ensure that security parameter settings set appropriately on all system components before they enter production. (PCI Requirement 2.2.4)

System administrators are responsible to ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI Requirement 2.5)

Non-console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

- Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.
- System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.
- Must include administrator access to web-based management interfaces.
- Use vendor documentation and knowledge of personnel to verify that strong cryptography is in use for all non-console access and that for the technology in use it is implemented according to industry best practices and vendor recommendations.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data (defined below) post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must not store of sensitive authentication data in any form after authorization (even if encrypted). Sensitive authentication data is defined as the following:

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- 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. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying Pan

Campbell County 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. A properly masked number will show at most only the first six and the last four digits of the PAN. This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale
(POS) receipts. Policies and procedures for masking the display of PANs must mandate the following: (PCI requirement 3.3)

- A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.
- PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN.
- All other roles not specifically authorized to see the full PAN must only see masked PANs.

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

In order to safeguard sensitive cardholder data during transmission over open, public networks, Campbell County Public Library will use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.). These controls will be implemented as follows: (PCI Requirement 4.1)

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. Weak encryption (for example, WEP, SSL version 2.0 or older) is not to be used as a security control for authentication or transmission. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: Use and Regularly Update Anti-Virus Software or Programs.

Anti-virus Protection

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

For systems considered to be not commonly affected by malicious software, Campbell County Public Library will perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. (PCI Requirement 5.1.2)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and be capable of as well as configured to generate audit logs. Anti-virus logs must also be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Steps must be taken to ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period. (PCI Requirement 5.3)

Requirement 6: Develop and Maintain Secure Systems and Applications

Risk and Vulnerability

Campbell County Public Library will establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

Risk rankings are to be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and

other systems that store, process, or transmit cardholder data. (PCI Requirement 6.1)

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. All applicable non-critical vendor-supplied security patches are installed within an appropriate time frame (for example, within three months). (PCI Requirement 6.2)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to Campbell County Public Library District's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

- Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)
- Privileges must be assigned to individuals based on job classification and function (also called "role-based access control). (PCI Requirement 7.1.3)

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (PCI Requirement 8.3)

Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.1.5)

Requirement 9: Restrict Physical Access to Cardholder Datta

Physically Secure All Areas and Media Containing Cardholder Data

All publicly accessible network jacks must have physical and/or logical controls to restrict access to the secure network by unauthorized personnel. (PCI requirement 9.1.2)

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.5)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)
- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.8)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

Protection of Payment Devices

Devices that capture payment card data via direct physical interaction with the card (such as swipe readers and any other payment terminals) must be protected. This protection must include preventing the devices from being tampered with or substituted. (PCI requirement 9.9)

Campbell County Public Library must maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI requirement 9.9.1)

- Make and model of all devices.
- Location of each device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.

The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI requirement 9.9.2)

Employees and contractors who interact with the payment devices must be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI requirement 9.9.3)

- Employees must verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices.
- Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
- Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).

Requirement 10: Regularly Monitor and Test Networks

Audit Log Collection

Campbell County Public Library will implement technical controls that create audit trails in order to link all access to system components to an individual user. The automated audit trails created will capture sufficient detail to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges. (PCI Requirement 10.2.2)
- All invalid logical access attempts (failed logins). (PCI Requirement 10.2.4)

- Any use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI Requirement 10.2.5)

Campbell County Public Library's log generating and collecting solution will capture the following data elements for the above events:

- User identification. (PCI Requirement 10.3.1)
- Type of event. (PCI Requirement 10.3.2)
- Date and time. (PCI Requirement 10.3.3)
- Success or failure indication. (PCI Requirement 10.3.4)
- Origination of event. (PCI Requirement 10.3.5)
- Identity or name of affected data, system component, or resource. (PCI Requirement 10.3.6)

Audit Log Review

Campbell County Public Library's systems administrators will perform daily review of the audit logs. This review may be manual or automated but must monitor for and evaluate: (PCI Requirement 10.6.1)

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs of all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The audit review must also check the logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment. (PCI Requirement 10.6.2)

Subsequent to log review, systems administrators or other responsible personnel will follow up exceptions and anomalies identified during the review process. (PCI Requirement 10.6.3)

Campbell County Public Library must retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, Online, archived, or restorable from backup). (PCI Requirement 10.7)

Requirement 11: Regularly Test Security Systems and Process

Testing for Unauthorized Wireless Access Points

At least quarterly, Campbell County Public Library will perform testing to ensure there are no unauthorized wireless access points (802.11) present in the cardholder environment. (PCI Requirement 11.1)

The methodology must be adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components.
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.).
- Wireless devices attached to a network port or network device.

To facilitate the detection process, Campbell County Public Library will maintain an inventory of authorized wireless access points including a documented business justification. (PCI Requirement 11.1.1)

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), the configuration must be capable of generating alerts to notify personnel. Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.10). (PCI Requirement 11.1.2)

Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), Campbell County Public Library will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be performed at a minimum quarterly and repeated until passing results are obtained, or until all "high" vulnerabilities as defined in PCI Requirement 6.1 are resolved. Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.1)

Quarterly external vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures). External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Scan reports must be retained for a minimum of a year. (PCI Requirement 11.2.2)

For both internal and external vulnerability scans, Campbell County Public Library shall perform rescans as needed to validate remediation of failures detected during previous scans, as well as after any significant change to the network. Scans must be performed and reviewed by qualified personnel. (PCI Requirement 11.2.3)

If segmentation is used to isolate the CDE from other networks, perform tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. These tests need to be done from multiple locations on the internal network, checking both for improper accessibility from the out-of-scope zones to the in-scope zone as well as the reverse. (PCI Requirement 11.3.4)

For all in-scope systems for which it is technically possible, Campbell County Public Library must deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. The change detection software must be integrated with the logging solution described above, and it must be capable of raising alerts to responsible personnel. (PCI Requirement 11.5.1)

For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system.

Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider). (PCI Requirement 11.5)

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors.

Security Policy

Campbell County Public Library shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1) CRITICAL TECHNOLOGIES

Campbell County Public Library shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies. (PCI Requirement 12.3.1)
- Authentication for use of the technology. (PCI Requirement 12.3.2)
- A list of all such devices and personnel with access. (PCI Requirement 12.3.3)
- Acceptable uses of the technologies. (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies. (PCI Requirement 12.3.6)
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity. (PCI Requirement 12.3.8)
- Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use. (PCI Requirement 12.3.9)

Security Responsibilities

Campbell County Public Library's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4) INCIDENT RESPONSE POLICY

The Systems Coordinator shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

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,

- Theft, damage, or unauthorized access (e.g., 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).
- Fraud – Inaccurate information within databases, logs, files or paper records.

Reporting an Incident

The Library Director should be notified immediately of any suspected or real security incidents involving cardholder data:

- Contact the Library Director to report any suspected or actual incidents. The library maintains procedures with its information technology coordinator and communications 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.
- No one should communicate with anyone outside of their supervisor(s) or the Library Director about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Library Director.
- Document any information you know while waiting for the Library Director to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response Policy (PCI requirement 12.10.1)

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.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

   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.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)
   d. Local authorities (if appropriate)

3. 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

4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Systems Coordinator will work with legal and management to identify appropriate forensic specialists.

5. Eliminate the intruder's means of access and any related vulnerabilities. 6.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 the Administration and 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.

Security Awareness

Campbell County Public Library shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Service Providers

Campbell County Public Library shall implement and maintain policies and procedures to manage service providers. (PCI requirement 12.8)

This process must include the following:

- Maintain a list of service providers. (PCI requirement 12.8.1)
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess. (PCI requirement 12.8.2)
- Implement a process to perform proper due diligence prior to engaging a service provider. (PCI requirement 12.8.3)
- Monitor service providers' PCI DSS compliance status. (PCI requirement 12.8.4)
- Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. (PCI requirement 12.8.5)

Bank Statements and Reconciliation Reports

Created 19 Jul 2000
Revised 19 Apr 2011
Reviewed 18 Dec 2024

The library bookkeeper 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 payments issued during the previous month, all deposits made in 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 18 Dec 2024

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 15 Nov 2017
Reviewed 18 Dec 2024

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

Charges and fees

Documentation from the library's automation system is provided to the library bookkeeper to verify receipts and deposits for all charges 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:

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

A separate "bank" amount of $150.00 is kept at each branch and is used only for making change for larger bills and replenishing the cash drawer when a large refund is paid to a patron.

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 bookkeeper for review.

Waivers

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

Safes

Created 15 Nov 2017
Revised 15 Nov 2017
Reviewed 18 Dec 2024

Each branch has a safe with a combination lock. Petty cash, excess cash from daily operations, and other cash funds will be kept in the closed/locked safe at all times. Cash drawer funds, change bank funds and all other cash funds are kept in other locked drawers when the library is closed.

All "on-hand" cash funds are kept to an absolute minimum through daily monitoring and regular donations.

Other important documents, such as system level passwords, may also be kept in a branch safe. Access to these documents should be cleared with the branch manager.

The branch manager and the patron services supervisor are the only staff members at each branch who are authorized to have access to the combination for the safes. The library bookkeeper maintains the combinations to all of the library's safes.

Staff Reimbursements for Purchases

Created 19 Jul 2000
Revised 14 Nov 2006
Reviewed 18 Dec 2024

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 ensure 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 library 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 18 Dec 2024

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 board 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 18 Dec 2024
Reviewed 18 Dec 2024

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 in its safe. Only branch managers should access these funds. Transactions should be reimbursed only with a receipt. At all times, total cash and receipts will equal $100.

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 the library bookkeeper.

The library director or the library bookkeeper may conduct an unscheduled check of all petty cash funds to ensure proper handling.

Library-Issued Credit Cards

Created 15 Jul 2003
Revised 19 Nov 2009
Reviewed 18 Dec 2024

Credit cards are issued to staff members who frequently make purchases for library events, have frequent travel expenditures, pay for services provided to the library, operate vehicles owned by the library, 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 bookkeeper regularly.

Balances on credit cards are paid in full by the library bookkeeper 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 their receipts. If the charges listed and receipts match, the statement is initialed and dated. The statement and receipts should then be sent to the library bookkeeper for payment.

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

Charges on the library director's library-issued credit card are reviewed by the board treasurer each month.

Fraud Prevention

Created 17 Nov 2009
Revised 17 Nov 2009
Reviewed 18 Dec 2024

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.