Pamunkey Regional Library Financial Policies

The Library Board establishes this financial policy to ensure fiscal responsibility, appropriate use of funds in support of the Library's Mission and Goals, and in compliance of appropriate laws and ordinances.

Audit Policy

1. Background

    a) Audit policy provides guidance on the selection of an independent accounting firm to provide opinions and/or reports on the Library's financial statements and internal controls in compliance with federal and state standards.

2. External Auditors

    a) External auditors will be selected to perform annual audits through a request for proposal (RFP) process every five years, unless otherwise approved by the Library Board. The Library may use the services of any of its four counties to facilitate this function.

    b) The Librarian's recommendation of an external auditor is reviewed and approved by the Finance Committee of the Board and referred to the Library Board for approval.

    c) Included under the scopes of services for external auditors is the issuance of any and all required opinions, internal control and compliance reports and management letters.

    d) Library assistance will be provided to external auditors, in order to produce timely and accurate financial statements and related audit opinions and reports.

Accounting Policy

1. Background

    a) An accounting policy addresses the accounting methods used and the manner in which revenues are collected/recognized and expenditures are disbursed/incurred.

2. Financial Statements

    a) The year-end financial statements shall be formulated based upon accounting standards.

    b) Monthly financial reports shall be presented to the Library Board.

3. Fund Accounting

    a) Accounts are organized on the basis of funds, each of which is considered to be a separate accounting entity.

b) Purchase orders, contracts and other commitments for expenditure of moneys are recorded in order to reserve that portion of the applicable appropriation.

4. Capital Assets

a) Capital assets shall be capitalized for unit costs greater than a $5,000 expenditure for which useful life exceeds five years and meets capital definitions of land, building, improvements to building, infrastructure or equipment.

b) Capital assets shall be depreciated over the estimated useful life of the asset using auditor accepted depreciation manners.

c) Capital assets will be disposed of through public auction or by donation to a governmental entity.

5. Check Disbursements and Bank Transfers

a) Two officers of the Library Board will sign all checks.

b) All disbursements of funds will have proper supporting documentation attached (e.g., vendor's invoice) and be filed in a manner to provide the proper audit trail to such disbursement.

c) All financial institutions utilized by the Library will have written instructions regarding Library authorizations for wire transfers, restrictions on accounts funds can be wired and other procedures that will mitigate unauthorized movement of funds (e.g., call-back to independent person, written confirmations, etc.).

6. Petty Cash

a) Petty cash locations shall be established at the Library Office and in all Branch Libraries.

b) Petty cash funds shall be maintained in order to provide timely reimbursement for expenses incurred by an employee and/or department that do not exceed $20 per transaction.

c) Internal controls shall be followed in ensuring that any assigned person with oversight over petty cash fund distribution performs such function with appropriate reconciliations, safeguarding of petty cash, and other control practices.

7. Record Retention

a) All records shall be retained in accordance with the State of Virginia's Library and Archives Public Records Management policies.

8. Warrants

   a) The Library Board authorizes payment of monthly bills by official action of approval of the warrants recorded in the minutes of Library Board meetings.

Budget Policy

1. Background

   a) The Library's budget policy addresses the process by which a budget is formulated from the proposed library request to Library Board's adoption, including the Capital Improvements Program and other issues presented to the Board during the budget process.

2. Budget Objectives

   a) The Library Board annually adopts budget objectives which are correlated to Library mission statement, long-range strategic plans and/or current Board priorities/initiatives. The budget objectives shall serve as the basis on which the budget is initially formulated.

3. Operating Budget

   a) The Library will prepare an overall proposed annual operating budget request based on the budget objectives.

   b) Local funding for each program is apportioned as follows:

      Branch Libraries: Cost of operation and maintenance paid for by the County where the branch is located.
      Bookmobile: Cost of operation and maintenance divided on a use basis.
      Centralized Services: Books and library materials, librarians and administrative office, delivery services and library collections staff and other operations, network and automated library system maintenance and operation, continuing education, supplies and other shared goods and services are divided on a per capita basis using most recent published population figures.

   c) The Library Board will review and approve the proposed operating budget and authorize the Librarian to submit the request to the Counties.

   d) The Librarian will prepare and submit an operating budget request to each of its four counties in compliance with the County's instructions and timetable.

   e) The Library will receive appropriations from each of the four counties and based on those appropriations and the adopted budget objectives the Librarian will prepare a revised operating budget.

4. Budget Adoption

a) The Library Board authorizes all operating expenditures and appropriates funds for those expenditures by adoption of the Library Budget.

b) The Library Board authorizes the Library Director to execute all contracts for which the Board has appropriated funds through adoption of the budget.

5. Capital Improvements Program(CIP) Requests

a) The CIP is a plan for capital expenditures and a means of funding facilities, equipment and vehicles with a unit cost greater than $50,000 during the next five fiscal years.

b) The Library will formulate CIP requests for inclusion in each of its Counties' CIP.

6. Budget Amendments

a) Library Board approval is required for budget amendments that increase the Library's total approved annual operating budget.

Credit Cards

1. Background

a) The Library may use a credit card to purchase goods and services if it is in the best interest of the Library to do so.

b) The Library will use the Credit Card Vendor whose rates and service are most advantageous to the Library, as determined by the Library Director.

2. Use

a) Credit card use will be administered by the Library Director and Administrative Assistant.

b) Credit cards will be used for official Library purchases only. Use of the card for personal items is not permitted, even if the Library will be reimbursed later.

c) Credit card balances will be paid in full monthly.

Fund Balance Policy

1. Background

a) The Library desires to maintain the financial operation of the Library in a manner consistent with sound financial management principles including maintaining a fund balance.

2. Use of Fund Balance

a) The Library will maintain a fund balance for purposes of unanticipated expenditures, to provide for cash flow reserves during the fiscal year due to the timing difference between the receipt of revenues and disbursement of expenditures, and to meet desired reserves.

b) The Library will designate part of the fund balance for anticipated, specific purposes such as purchase of Library vehicles, upgrades to Library technology, matching grant funds, payout of leave balances and other special projects.

c) The Library Board authorizes all expenditures and appropriates funds for those expenditures from the Library's fund balance by official action recorded in the minutes of Library Board meetings.

Investment and Deposits Policy

1. Background

a) The Library will deposit its funds in a bank selected through an RFP process.

b) The Library will transfer all funds, except those needed for immediate use, from the bank into the Local Government Investment Pool maintained by the Commonwealth of Virginia or an interest bearing investment account which offers the equal security and greater return.

c) In recognition of its fiduciary role in the management of all public funds entrusted to its care, it shall be the policy of the Library that all investable balances be invested with the same care, skill, prudence and diligence that a prudent and knowledgeable person would exercise when undertaking an enterprise of like character and aims under circumstances prevailing at that time.

2. Investment Objectives

a) Safety - the safeguarding of principal shall be the foremost objective of the investment program by mitigating credit risk and interest rate risk with all other objectives subordinated to the attainment of this objective.

b) Liquidity - the investment portfolio shall be managed at all times with sufficient liquidity to meet all daily and seasonal needs, as well as special projects and other operational requirements either known or which might be reasonably anticipated.

c) Yield - the investment portfolio shall be managed with the objective of obtaining no worse than a fair value rate of return over the course of budgetary and economic cycles, taking into account the constraints contained herein and the cash flow patterns of the Library.

3. Library Internal Controls

a) The Library shall maintain a system of internal controls which shall be documented and reviewed with internal and independent auditors and meet the requirements of the Government Accounting Standards Board.

b) These controls shall be designed to provide reasonable assurance to prevent losses of public funds due to fraud, error, misrepresentation, unanticipated market changes or imprudent actions.

Pamunkey Regional Library PCI Compliance Policy

Who Should Read this Policy: All persons who have access to credit card information, including:

- Every employee that accesses handles or maintains credit card information. Pamunkey Regional Library employees include full-, part-time and hourly staff who access, handle or maintain records.
- Employees who contract with service providers (third party vendors) who process credit card payments on behalf of the Library.
- Employees who manage programs and events and require payment processing capabilities.
- IT staff responsible for auditing Library systems to ensure no credit card numbers are stored electronically.

Name: PCI DSS stands for Payment Card Industry Data Security Standard. PCI DSS is a global security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

Purpose: The PCI DSS represents a set of comprehensive requirements for enhancing payment account data security. The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS includes technical and operational requirements for **security management, policies, procedures, network architecture, software design and other critical protective measures** to prevent credit card fraud, hacking and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

Reason for the Policy: The standards are designed to protect cardholder information of patrons, parents, donors, customers and any individual or entity that utilizes a credit card to transact business with the Library. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.

Entities Affected by this Policy:

- All areas that collect, maintain or have access to credit card information. These currently include:
    - All branches and departments who have relationships with third party vendors that serve as access points through which Elavon, EnvisionWare, or any other payment services approved by the Library are reached. These departments must confirm PCI compliance on the part of the vendor. This category includes any processing performed that does not use the Library's merchant accounts.

Third Party vendors that process and store credit card information for Pamunkey Regional Library using the Library's merchant account(s) include:

- Verifone and EnvisionWare

Definitions:

Merchant – Any organization that accepts credit cards for payment. Merchant is not a commerce definition but rather a definition of any for profit or non-profit entity that facilitates payments from patrons or customers via credit card.

Merchant Account - A relationship set up between the Library and a processor in order to accept credit card transactions. Merchant accounts fall into two (2) categories:

- **Card Present**, which are used for terminals
- **Card not Present**, which is used for web payment of fines and fees.

Merchant Accounts are designated for deposit into a bank. All merchant accounts can deposit into one bank account or each Merchant Account can be deposited into different bank accounts.

Financial Data Manager (FDM) – The Business Operations Manager of the Library who has oversight responsibility for this policy. The Financial Data Manager will also communicate changes to the Library Director and Supervising Librarians in order to facilitate enforcement of the policy.

The FDM will be responsible for staying abreast of changes to PCI DSS requirements, suggesting updates to the policy, coordinating training of entities.

Credit Card Data - Full magnetic stripe or the PAN (Primary Account Number) plus any of the following:

- Cardholder name
- Expiration date
- Service Code (3 or 4-digit number on cards that use a magnetic stripe)

PCI-DSS - Payment Card Industry Data Security Standard

PCI Security Standards Council - The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

Self-Assessment - The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS. This policy is written in adherence to SAQ-P2PE-HW

PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

Level of Compliance: Credit card companies and financial institutions validate that merchants (PRL) are rated based on their volume of transactions. The rating that a company receives determines the process that they must go through in order to be validated.

There are four levels of PCI Compliance:

- Level 1: 6,000,000 card transactions per year
- Level 2: 1,000,000 to 6,000,000 card transactions per year
- Level 3: 20,000 to 1,000,000 card transactions per year
- Level 4: Less than 20,000 card transactions per year.

Level 1 is the most stringent and level 4 is the least stringent. If a merchant (PRL) suffers an attack that has caused account data to be compromised, the *merchant level requirement* goes up to level 1 automatically. Based on the number of credit card transactions processed annually across the Library system (fewer than 20K per year), and the fact that the Library has not experienced a breach, Pamunkey Regional Library would be classified as **Level 4**.

PCI DSS Version 3.2.1 Requirements:

1. Library policy prohibits the storing of any credit card information in an electronic format on any computer, server or database (this includes Excel spreadsheets).
2. Library policy prohibits the emailing, messaging, chatting or faxing of credit card information.
3. Library policy prohibits types or handwritten activities and the transmission or storage of any written cardholder PANs.

The following list communicates the full scope of the compliance requirements applicable to the Library's card processing systems.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Procedures:

Pamunkey Regional Library requires compliance with PCI standards. To achieve compliance, the following requirements must be met:

General Requirements:

- Credit card merchant accounts must be approved by the Library Director.

- Management and employees must be familiar with and adhere to the PCI-DSS requirements of the PCI Security Standards Council.
- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and be approved by the Financial Data Manager.
- A list of card processing terminals must be maintained and updated as needed indicating the serial number and physical location of each device, firmware version and hardware version.
- Any new terminal received by the Library must be kept locked in a secure location until deployment.
- Any terminal requiring service or replacement must be tracked at all times and shipped via a method that provides shipment tracking.
- Terminals must be physically inspected at least annually as well as at any time that staff or patrons/customers identify a concern with a suspected terminal.
- Management must conduct an annual self-assessment against the requirements and submit results to the Financial Data Manager.
- The Financial Data Manager must create or confirm the existence of appropriate policies and procedures for credit card processes, storage, and destruction of card data.
- Job descriptions for employees with access to credit card data must be reflective of this access and must include data security requirements associated with access.
- Access to the cardholder data environment must be restricted to only those employees with a need to access and physical controls must be in place to protect the cardholder data environment.
- Terminals/readers must be routinely examined for evidence of tampering and any evidence brought to the attention of the Compliance Coordinator.
- **Pamunkey Regional Library prohibits anyone from accepting credit card information or processing credit card payments on behalf of the patron/customer.**

Breach or Suspected Breach / Reporting

- In the event of any suspected breach, the Library Director, Financial Data Manager, and EnvisionWare support (888-409-0888) must be notified immediately, not more than 4 hours after detection.
- All details about a suspected breach must be carefully documented including the time and number when the Library Director and Financial Data Manager are notified and the support representative and Support Case number when notifying EnvisionWare.
- If there is any suspicion of an integrity problem with the system, the Library should evaluate disabling the system until the breach can be researched.
- All staff, patrons/customers, managers and EnvisionWare personnel involved in the breach response must be documented carefully.
- The Financial Data Manager will track EnvisionWare's response to a suspected breach to ensure that it receives a timely response and follow-up.
- The Financial Data Manager must be immediately notified regarding any physical damage, abuse, removal or modification of any terminal.

Storage and Disposal

- Credit card information must not be entered/stored on any electronic device - this includes Library network servers, workstations, laptops, tablets and cell phones- unless it is explicitly approved for use as part of the cardholder data environment.
- Credit card information must not be transmitted via email, SMS, chat or fax
- Credit Card payments must be processed using EnvisionWare's system only by patrons or customers. Credit card numbers must NOT be entered into a web page of a server hosted on the Pamunkey Regional Library network.
- Any paper documents containing credit card information should be avoided unless a specific situation requires documenting, in which case the documentation must be limited to information required to transact business, those individuals who have a business need to have access, should be in a secure location, and any paper must be destroyed via cross-cut shredding or placement in a secure shred bin once business needs no longer require retention.
- All credit card processing components must be programmed to print-out only the last four or first six characters of a credit card number.

- Sensitive cardholder data must be destroyed when no longer needed for reconciliation, business or legal purposes. In no instance shall this exceed 45 days and should be limited whenever possible to only 3 business days. Secured destruction must be via cross-cut shredding in house or with a third-party provider with certificate of disposal.
- Neither the full contents of any track of the magnetic stripe nor the 3-digit or 4-digit card validation code may be stored in a database, log file, electronic document or point of sale product.

Third Party Vendors (Processors, Software Providers, Payment Gateways, or Other Service Providers)

- The Financial Data Manager has approved the EnvisionWare system as the only system that is engaged in, or proposes to engage in the processing of transaction data on behalf of Pamunkey Regional Library regardless of the manner or duration of such activities.
- For card present transactions, the EnvisionWare system accepts cardholder data only into an EnvisionWare-provided credit card terminal, which is entered only by patrons/customers whereupon it is encrypted into a specially encrypted packet that is then transmitted via a SSL (TLS1.2) connection to the gateway via Library's network to the EnvisionWare-provided Verifone POINT gateway service. No Library computers are used for entry of cardholder data. *The only PCI in-scope component is the credit card terminal*.
- The Financial Data Manager must ensure that all third-party vendors adhere to all rules and regulations governing cardholder information security.
- The Financial Data Manager must contractually require that all third parties involved in credit card transactions meet all PCI security standards, and that they provide proof of compliance and efforts at maintaining ongoing compliance.
- Information must be maintained about which PCI-DSS requirements are managed by each third party provider and which are managed by Pamunkey Regional Library.

Additional Requirements:

- Complete an annual PCI assessment
    - Assessment for terminal (card present) transactions (SAQ-P2PE-HW)
- Without adherence to the PCI-DSS standards, the Library would be in a position of unnecessary reputational risk and financial liability. Merchant account holders who fail to comply are subject to:
    - Any fines imposed by the payment card industry
    - Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees
    - Suspension of the merchant account
    - The Library maintains breach protection coverage through the EnvisionWare solution.

Self-Assessment

- The PCI-DSS Self-Assessment Questionnaire must be completed at the Library level by the merchant account owner annually and anytime a credit card related system or process changes.

Additional Resources

PCI Security Standards Council https://www.pcisecuritystandards.org

Purchasing Policy

1. Background
    a) The Pamunkey Regional Library Board affirms its intent to comply with the Virginia Public Procurement Act and adopts the following limits for purchasing with the Library Director designated as Purchasing Agent for the Library.

2. Summary of Purchasing Policy
    a) Purchase Classifications:
        - Single informal quote (fax, e-mail or telephone) required for purchases up to $2,500.
        - Two informal quotes required for purchases of $2,500.01 to $5,000.
        - Three informal quotes required for purchases of $5,000.01 to $15,000.
        - Three formal written quotes required for purchases of$15,000.01 - $30,000
        - Sealed bids or proposals and public posting required for purchases in excess of $30,000.01
        - Sole source requires written justification.

Revenue Policy

1. Background
    a) To ensure strong fiscal management practices, the proper controls over revenues is imperative in determining budget, forecasting, reconciliations, accounts receivable management and general oversight over the various revenues the Library collects.

2. Internal Controls
    a) All aspects of revenue recordation and cash receipt shall be subject to

proper internal controls as recommended by the Library's external auditors.

Travel Policy

1. Background

   a) Travel policy is intended to define for Library employees, and members of the Library Board, the manner in which travel shall be conducted and how funding and/or reimbursement for such travel expenditures will be handled.

   b) Library business for the purpose of this travel policy includes conferences, seminars, workshops, hearings, education, conventions and business meetings which benefit the Library.

   d) Any exceptions to this policy shall require the authorization of the Library Director.

2. Reimbursable Expenses

   a) Per Diem Allowance

      i) The traveler shall be allowed a daily per diem allowance equivalent to the Internal Revenue Service rate for the destination locality.

      ii) The employee should make a reasonable determination as to what portion(s) of the per diem allowance (i.e., breakfast, lunch and/or dinner) is applicable on the days in which traveling to/from destination occurs, with the Library Director also reviewing for reasonableness.

   b) In determining the reimbursable expenses for lodging and transportation, the actual costs of such lodging and transportation will be used as long as they are cost effective and reasonable, otherwise a calculated reasonable cost will be used as the basis for reimbursement.

3. Local Mileage Reimbursement

   a) The local mileage reimbursement rate shall be equal to the Internal Revenue Service allowable rate to be updated annually.