Approved by the Board of Trustees March 27, 2025

St. Joseph Public Library
Cybersecurity Policy

As a state funded and locally tax supported government agency, the St. Joseph Public Library (SJPL) is entrusted with the duty of collecting sensitive and personal information about library staff and patrons. SJPL takes reasonable cybersecurity and other measures to safeguard information including Personally Identifiable Information (PII) and other types of information. This also includes information a Federal agency or pass-through entity designates as sensitive or other information the recipient or subrecipient considers sensitive and is consistent with applicable Federal, State, local, and tribal laws regarding privacy and responsibility over confidentiality. (CFR 200.303)

Credit cards are accepted for the payment of fees and SJPL complies with the Payment Card Data Security Standard (PCI-DSS).

The SJPL Confidentiality of Patron Records Policy provides specifics about protecting the privacy of patron data.

As a member of the Missouri Evergreen Consortium (MEC), whose libraries constitute an interconnected or combined system to enable collaboration, SJPL supports and abides by the Missouri Evergreen Policy on Personally Identifiable Information. SJPL's Cybersecurity Policy is to be used concurrently with the Missouri Evergreen Policy on Personally Identifiable Information and the SJPL Confidentiality of Patron Records Policy.

SJPL contracts with a Managed Service Provider (MSP) to manage the library's IT infrastructure. The MSP provides IT services, security, data management, assists with compliance, manages staff access, and provides a help desk for staff. The MSP also provides Endpoint Detection and Response for the SJPL network.

SJPL requires staff to have complex passwords.

SJPL provides security training to all staff, including policy awareness and cybersecurity best practices.

Administrative Procedure

This policy applies to all employees, full-time and part-time, temporary and permanent, and contractors and consultants who are on site. Volunteers will not be given access to patron or staff personal information.

All handling of patron records and card processing activities and related technologies will comply with this policy. Additionally, patron records are defined as personally identifiable information about an individual who has used any library service or borrowed any library materials.

The Library Director is designated to oversee the SJPL Cybersecurity Policy. They will address potential internal and external security risks to the security, confidentiality, and integrity of

personal information that could result in a compromise. SJPL has identified internal and external risks and is taking steps to mitigate them.

Internal Risks:

- Personal information deliberately or inadvertently given to someone via library staff. This risk is addressed in the following ways:

    - Through employee training and SJPL management. Library Managers, under the direction of the Library Director, are responsible for ensuring that this policy is communicated to SJPL staff and that staff comply with this policy in the course of their duties.

    - Upon employment with SJPL, newly hired employees will be trained on information security policies and procedures with refresher training offered periodically online and during staff development sessions.

    - Patron records, and any related paper records, will be stored securely and destroyed adhering to record retention policies.

    - Cardholder records require the cardholder's legal name, current address, and a current phone number and/or email address to communicate account information to the patron. Library cardholders are assigned a unique four-digit Personal Identification Number to access their cardholder account online. Library staff do not have access to this number but can send a reset link to the patron.

    - In accordance with the SJPL Library Card Policy, cardholders are responsible for ensuring that their account information is accurate and up to date. Accounts for those age 17 and younger require a parent or legal guardian to assume responsibility for items checked out and as such, account information is accessible to said parent or legal guardian.

    - All candidates for employment with SJPL are hired contingent on a successful background check. Volunteers ages 18 and older are also subject to background checks.

    - Applications for employment and background check information are securely stored and subsequently destroyed based on a record retention schedule. Applications for employment for those who are not hired are also stored and destroyed according to a record retention schedule.

- Access to personal information via a staff computer. This risk is addressed in the following ways:

    - Through staff training and management. Only authorized users of SJPL equipment will have access to workstations and software where information is stored. Authorized users include library staff members and contract employees.

    - SJPL requires logins and passwords for staff members on library computers.

    - Patrons are not permitted access to staff computers under any circumstances.

    - Volunteers will be provided access to staff computers only when those computers do not contain, nor provide access to patrons' confidential information.

    - Before any equipment that stores confidential information is discarded, sold, or returned, SJPL will make certain the hard drives are secured or completely erased.

External Risks:

- Access to personal/patron information via an outside computer or other outside source. This risk is addressed in the following ways:

    - For the Missouri Evergreen Consortium, this is done via third party vendors which are configured to protect cardholder data. SJPL also maintains a local firewall to protect against external intrusion. Unique logins and passwords are required for access to patron information.

    - Antivirus software is maintained and regularly updated, and regular security system checks are conducted.

    - All third-party providers and vendors are required to uphold the SJPL Cybersecurity Policy.

Breach of Security:

While SJPL has put into place physical, electronic, and managerial procedures in an effort to safeguard and secure information collected to prevent unauthorized access, to maintain data security, and to ensure the correct use of information, SJPL cannot guarantee that information collected will never be accessed by unauthorized users.

Any security breach or suspected security breach of confidential information must be reported immediately to the Library Director and contract IT Service company. The IT Service company will investigate and respond to any suspected intrusion or failure and notify staff of the situation.

Staff must notify their supervisor immediately if secure information, including passwords and confidential information is lost, stolen, or shared (inadvertently or otherwise), or suspected of being lost, stolen, or shared.

The Library Director will take disciplinary action where appropriate, when and if an error on the part of specific SJPL staff member(s) are involved in the breach.

The Library Director will communicate with any impacted patrons and/or staff members. This will include notification of the breach and what steps, if any, SJPL will take to remedy the situation for the patron or staff member as well as what steps they should take to further ensure the safety of their information.