MARSHALL PUBLIC LIBRARY - CYBER SECURITY POLICY

Approved by the Marshall Public Library Board of Trustees: 04/08/2025

As a state-funded and locally tax-supported government agency, the Marshall Public Library (MPL) is responsible for safeguarding sensitive and personal information about library staff and patrons. The Library is committed to protecting information within its systems and services from unauthorized disclosure, modification, or destruction, whether accidental or intentional. MPL will comply with all applicable federal and state regulations regarding personal information systems and federal grant awards (CFR 200.303). Additionally, because the Library accepts credit card payments, MPL will comply with the Payment Card Industry Data Security Standard (PCI-DSS).

As a member of the Missouri Evergreen Consortium (MEC), which enables collaboration among interconnected library systems, MPL supports and adheres to the Missouri Evergreen Policy on Personally Identifiable Information. The Library's Information Security Policy is to be used in conjunction with the Missouri Evergreen Policy on Personally Identifiable Information.

ADMINISTRATIVE PROCEDURE

This policy applies to all employees, whether full-time, part-time, temporary, or permanent, as well as contractors and consultants working on-site. Volunteers will not be granted access to patron or staff personal information.

All handling of patron records, card processing activities, and related technologies must comply with this policy. Patron records include personally identifiable information about individuals who have used any library service or borrowed any library materials.

The Library Director and Assistant Director are designated to oversee the Library's Information Security Policy. They will assess and address potential security risks to ensure the security, confidentiality, and integrity of personal information.

INTERNAL RISKS - PERSONAL INFORMATION DISCLOSURE BY LIBRARY STAFF

Risk is mitigated through employee training and library management oversight. The Library Director and Assistant Director will ensure that all staff members are informed of this policy and comply with it in their daily responsibilities.

Newly hired employees will receive training on information security policies and procedures upon employment, with periodic refresher training provided during staff development sessions.

Patron records, including paper versions of library card applications, will be securely stored and destroyed upon record purging from MEC.

Cardholder records must include the cardholder's legal name, current address, and current phone number and/or email address for account communication. Each library cardholder is assigned a Personal Identification Number (PIN) to access their account online; library staff do not have access to these numbers but can send a reset link.

In accordance with MPL's Cardholder Policy, cardholders are responsible for keeping their account information accurate and up to date. The Library will provide account information about a minor child only to their parent, guardian, or custodian.

Employment applications will be securely stored and destroyed after six months. Applications from individuals not hired by MPL will be treated in the same manner.

A breach of confidentiality regarding personal information may result in disciplinary action, up to and including termination.

ACCESS TO PERSONAL INFORMATION VIA STAFF COMPUTERS

Risk is mitigated through staff training and access management. Only authorized users, including Library staff and contract employees, will have access to workstations and software containing confidential information.

MPL requires unique logins for staff members on work terminals, with password protection on all staff terminals.

Patrons will not be permitted access to staff terminals under any circumstances. Volunteers will be granted access only to terminals that do not contain or provide access to confidential patron information.

Authorized users must report any loss, theft, or unauthorized sharing of secure information (including passwords) to the Library Director immediately.

All computers, laptops, and mobile devices must be locked when unattended. Mobile devices must be stored securely in locked staff areas when not in use.

Before disposing of, selling, or returning any equipment storing confidential information, MPL will ensure that all hard drives are either secured or completely erased.

EXTERNAL RISKS
ACCESS TO PERSONAL/PATRON INFORMATION VIA AN OUTSIDE COMPUTER OR OTHER SOURCE

Risk is managed through third-party vendors configured to protect cardholder data. MPL will maintain a local firewall to prevent external intrusion and require unique logins and passwords for access to patron information.

MPL will ensure that antivirus software is updated regularly and that security system checks are conducted periodically.

The Library will contract only with vendors capable of maintaining appropriate safeguards for patron information. Default vendor-supplied passwords and security parameters will not be used.

All third-party providers and vendors must uphold MPL's Information Security Policy.

BREACH OF SECURITY

MPL has implemented physical, electronic, and managerial procedures to safeguard collected information, prevent unauthorized access, maintain data security, and ensure correct usage. However, no system can guarantee complete protection from unauthorized access.

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

The Library Director will take appropriate disciplinary action if a breach results from staff error.

The Library Director will communicate with any impacted patrons and/or staff members, including notification of the breach and the steps MPL will take to address the situation.

By adhering to this Cyber Security Policy, Marshall Public Library ensures that patron and staff information remains secure, confidential, and protected from unauthorized access or misuse.

Approved by the Board of Trustees of the Marshall Public Library on [date].