MID-HUDSON LIBRARY SYSTEM

103 Market Street
Poughkeepsie, New York 12601-4028
Phone: 845.471.6060
Fax: 845.454.5940
http://midhudson.org

Technology and Data Security Policy

General

Data Security, Privacy & Confidentiality

MHLS is committed to secure data, privacy, and confidential treatment of personal and private data. Our goal is to enforce the confidential management of the data as well as to maintain integrity in all record, transactional and statistical data. This includes:

- **Staff Training**: conduct regular, ongoing training for MHLS staff and member library staff who have access to data in MHLS managed software.
- **Privacy Audits**: Conducting regular privacy audits. This helps to verify that all MHLS processes and procedures comply with privacy policies and that user access is regularly reviewed.
- **Phishing Audits**: Conduct periodical test with staff to test reactions to email phishing campaigns.
- **Response Plans**: Creating and regularly reviewing response plans for ILS data incidents. Examples of these incidents could be data breaches or leaks. The response plan should include communications to staff and affected users. The response plan should also include what steps to take to remedy and/or mitigate the damage from the incident.

Definitions

(a) "Personal information" shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person;

(b) "Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

i. social security number;

ii. driver's license number or non-driver identification card number;

103 Market Street
Poughkeepsie, New York 12601-4028
Phone: 845.471.6060
Fax: 845.454.5940
http://midhudson.org

iii. account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;

iv. account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

v. biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity;

vi. a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

Safeguarding Data Privacy

A. MHLS Employees and member library staff and volunteers, including board members must be mindful of and respect data privacy at all times; safeguarding the access to and distribution of personal and private information collected, stored or available to them. Data should only be used in ways that will keep identity and the confidentiality of information secure. Patron record information and identifiable transactions are mandated to be kept confidential as per New York State Law and should not be transmitted, shared, published, or made accessible to any third party without proper authorization. Employees shall conform to all applicable laws and regulations.

i. **Internet Security:** Access to MHLS files, servers and data will be limited to only those individuals that require access to complete assigned tasks and manage services.

ii. **Data Storage:** All work completed by MHLS staff will be stored in the designated cloud environment rather than on local hard drives or removable storage. Items stored in cloud directories can be accessed from any device, they are secured by password protection, levels of authorized access and backed up regularly. File

103 Market Street
Poughkeepsie, New York 12601-4028
Phone: 845.471.6060
Fax: 845.454.5940
http://midhudson.org

access will be facilitated by the IT Supervisor or Technology Operations Manager and approved by the Executive Director and/or the Technology Operations Manager.

iii. **Passwords:** Personal passwords should not be shared with others nor made available in open areas. Passwords should be changed regularly (once every 180 days at minimum), and follow guidelines posted on staff.midhudson.org

iv. **Internet Security:** Employees should be using a secure and password protected internet connection (Wi-Fi) and a secure updated browser when accessing, processing, or storing critical and protected data. Internet Security best practices will be routinely shared with staff. Antivirus protection is installed on MHLS owned devices.

v. **Email Security:** Email security is taken seriously at MHLS.

i. MHLS will complete regular security awareness education, and complete follow up retraining.

ii. MHLS staff will avoid sending personal information when possible and limit the recipients of the email to only those individuals who require and are appropriately vetted to receive the information. When sending personal identifiable information in email MHLS staff will use encrypted email, in accordance with New York State Article 39-F Notification of Unauthorized Acquisition of Private Information; Data Security Protections. SECTION 899-AA Notification; person without valid authorization has acquired private information (https://www.nysenate.gov/legislation/laws/GBS/899-AA)

B. Software Copyright and Licensing: MHLS is obliged to adhere to the terms of software usage agreements and employees should be made aware of any usage restrictions. Software and policy changes can be completed through an email request to techsupport@midhudson.org

C. Report Security Incidents: All employees are required to report data security incidents or any indication that malicious malware has inadvertently been imported into employee workspaces or equipment. Contact your supervisor and Techsupport@midhudson.org immediately to report these incidents.

D. Access to Equipment: MHLS owned equipment can be requested and signed out for remote use, including for long-term use by staff who have an approved, formal telecommuting agreement. MHLS will loan inspected equipment only. The equipment will be signed out using the approved form which identifies the borrowed equipment specifically. The equipment is intended for MHLS business operations and not for personal use. The individual who borrows the equipment is responsible for maintaining a secure and safe environment for the use of the equipment,

103 Market Street
Poughkeepsie, New York 12601-4028
Phone: 845.471.6060
Fax: 845.454.5940
http://midhudson.org

including access to data and processes. The equipment should not be altered in any way and should be returned in a condition relative to when it was issued. Requests for equipment will be based on availability and priority to the organization. Equipment that has been signed out may be recalled at any time and must regularly be returned for security and other updates.

Management of Integrated Library System (ILS)

A. Collection & Retention of User Data: MHLS will collect and store only the necessary data required for internal operations the information required to provide a service or meet a specific operational need. MHLS respects §4509 of New York State's Civil Practice Law & Rules[1] and supports the Library Bill of Rights[2] and will advocate on behalf of patron confidentiality with vendors to develop methods which are secure and retain anonymized data where possible and reduce data retention to meet only the immediate needs of the transaction or processes within the ILS.

MHLS does not collect:

i. Government or organization issued identification numbers (e.g. Social Security Numbers, Alternative ID, Driver's License Numbers) will not be used in patron records.
ii. Patron usage of database searches
iii. Individual member library computer use or interlibrary loan requests for materials outside of the systems.
iv. Demographic information (e.g. gender identity, race/ethnicity, employment). Any recommendations or requirements for this information have been removed by the Directors Association and are reflected in the policy document Resource Sharing Standards
v. MHLS central authentication does not create data that identifies identifiable patron usage.
vi. It is the responsibility of library and system staff to purge their individual email and/or user files.
vii. MHLS has the responsibility of protecting the privacy of our patrons in accordance with New York State Law. Library records, as defined by §4509 of New York State's Civil Practice Law & Rules[1], should not be released or made available in any format to a federal agent, law enforcement

[1] https://www.nysenate.gov/legislation/laws/CVP/4509
[2] https://www.ala.org/advocacy/intfreedom/librarybill

103 Market Street
Poughkeepsie, New York 12601-4028
Phone: 845.471.6060
Fax: 845.454.5940
http://midhudson.org

officer or other person unless a court of competent jurisdiction has entered a court order in proper form.

Therefore, we will do our utmost to uphold the privacy and confidentiality of patrons' free access to information while responding to legitimate security concerns.

B. Third-Party Vendors: MHLS uses third-party vendors to provide digital collections, streaming media content and more. Some of these vendors may collect and share the information you provide to them to use their services. Patrons may choose not to use these third-party vendors.

i. MHLS manages third party access to the ILS Application Program Interfaces (APIs) and reserves the right review the vendor's security measures and limit access accordingly.

ii. MHLS reserves the right to review API access and eliminate access to some or all data points.

iii. MHLS reserves the right to require vendors to attest to limiting access or use of data retrieved through API access.

iv. In relation to the types of information that could be collected by the vendor:

a. Request for information to enhance patron experience or create shared content may not be shared without explicit permission on all data points and usage.

b. MHLS not share, post or export Internet Address (IP Address), search history, location-based data, and device information created by third party vendors.

c. Only non-personally identifiable information, such as ad views, analytics, browser information, cookie data, date/time of request, demographic data, hardware/software type, interaction data, serving domains, page views, and the web page visited immediately prior to our site will be collected for local use only.

d. Other data, as described in the vendor's privacy policy and terms of use may have "restricted for your use" and "limited to the period of the contract".

ii. **Third-party Integrations and ILS Application Program Interfaces (APIs)**

a. MHLS will review any API access from third party vendors and reserves the right to deny access to vendors who will not:

103 Market Street
Poughkeepsie, New York 12601-4028
Phone: 845.471.6060
Fax: 845.454.5940
http://midhudson.org

i. Provide a statement of data use

ii. Provide a privacy, retention breach policy upon request

iii. Provide examples of data requests for approval and limit all data requests to only those examples that have MHLS approval.

b. MHLS reserves the right to require API access through a validated key that can be tracked for access.

i. MHLS reserves the right to determine and limit the API profile and access in the following ways:

- Set expiration for regular renewal review
- Access to record types and fields

c. All transmission of patron data must be encrypted and secure.

C. Data Integrity and Security

i. Encryption: MHLS patron transaction and authentication data must be encrypted in storage and whenever data is transmitted to and from the ILS. Examples of storage and transit include staff desktop clients, web browsers, and mobile apps. Encryption methods should follow up-to-date security protocols and practices.

ii. **Static IP:** MHLS requires that all access to the shared ILS be completed through an approved static Internet Protocol (IP) or Virtual Private Network (VPN)

iii. Patron PINs & Passwords:

a. MHLS uses encrypted Patron PINS to not be viewable by staff. This protects the access to patron reading history and other lists that are private, not transaction related, and required to be viewed by only the patron themselves.

b. MHLS makes available encrypted and secure authentication and encourages all member libraries to use only Encrypted and Secure authentication.

c. MHLS will not provide unencrypted PIN access to third parties and does not recommend or support vendors who require access to the patron record through Barcode/PIN access.

103 Market Street
Poughkeepsie, New York 12601-4028
Phone: 845.471.6060
Fax: 845.454.5940
http://midhudson.org

iv. Notifications & Reports

a. MHLS supported, ILS generated user notifications for holds, overdue items, and bills contain minimal personal data. These notifications include email, text messages, and automated phone calls.

b. Access to ILS reports is limited to authorized member library staff. Member library Directors determine the level of access provided to their staff. ILS reports should contain only the minimum amount of personal data necessary for operational needs. Reports intended for wider distribution should be de-identified. This can be done by removing personal data or aggregating personal data to ranges or groups that can't easily be re-identified.

D. Third-party Integrations and ILS Application Program Interfaces (APIs)

E. ILS Cloud Hosting Security and Privacy

i. MHLS will request and review ILS data security and privacy practices, reserve the right to eliminate or block security risks without prior notification.

ii. Security involves both managerial and technical measures to protect against the following:

a. Loss

b. unauthorized access

c. destruction

d. use

e. disclosure of data

f. Provide up to date compliance with

F. ILS Patron Records and Transactional Data:

i. All data that is posted must be anonymous including training examples and posted reports.

ii. Exported reports should exclude identifying patron information when possible.

iii. Comprehensive lists or reports that include identifying patron data points may be sent only to a library director.

iv. Any patron data exported should be stored securely and purged as soon as necessary processes with the data are completed.

Board Approved: September 2022