Systems Access and Data Handling Policy

Purpose

Protecting patron privacy and confidentiality is a core principle of librarianship. The American Library Association's Library Bill of Rights, Article VII, states that:

> *[a]ll people, regardless of origin, age, background, or views, possess a right to privacy and confidentiality in their library use. Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information.*[1]

Patrons' right to confidentiality in the library is codified in New York State Civil Practice Law & Rules, Section 4509: Library records:

> *Library records, which contain names or other personally identifying details regarding the users of public, free association, school, college and university libraries and library systems of this state, including but not limited to records related to the circulation of library materials, computer database searches, interlibrary loan transactions, reference queries, requests for photocopies of library materials, title reserve requests, or the use of audio-visual materials, films or records, shall be confidential and shall not be disclosed except that such records may be disclosed to the extent necessary for the proper operation of such library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.*[2]

[1] ALA Library Bill of Rights, http://www.ala.org/advocacy/intfreedom/librarybill

[2] New York Civil Practice Law, Sec. 4509, Library Records, https://newyork.public.law/laws/n.y._civil_practice_law_section_4509#:~:text=Library%20records%2C%20which%20contain%20names,library%20materials%2C%20computer%20database%20searches%2C

The Pioneer Library System acknowledges its responsibilities to protect patron confidentiality in its Confidentiality of Library Records Policy[3].

The Pioneer Library System also acknowledges its responsibilities under New York's Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") to develop, implement, and maintain reasonable security safeguards to prevent the unauthorized release of personal information.

Definitions

Personally Identifiable Information (PII)

Patron PII is generally data about a patron. Examples include a patron's name, address, email address, telephone number, or date of birth, either alone or in combination. Additional data about patrons, data about activity that can be tied back to a patron, is also collected and stored in PLS Systems and should also be considered confidential. Examples of these types of data include a patron's circulation history, hold requests, or paid bills. For the purposes of this policy, the term "patron PII" describes all confidential information about a patron whether or not it is traditionally considered PII.

Integrated Library System (ILS)

The ILS supported and maintained by Pioneer Library System is Evergreen.

Pioneer Library System Systems

Systems maintained by Pioneer Library System, including those that may contain patron PII. These include, but are not limited to email, the ILS, the PLS reporting tool, LibCal, and Prefab Websites.

Scope

This policy shall apply to all individuals authorized to access PLS Systems as necessary for their job functions.

Accounts and Passwords

This portion of the policy establishes both that adequate controls on accounts and that appropriate password management and construction are important aspects of maintaining the security of systems that hold patron PII and protecting patron confidentiality.

---

[3] Pioneer Library System, Confidentiality of Library Records Policy, https://docs.owwl.org/pub/Community/SystemPolicies/Confidentiality%20of%20Library%20Records%20Policy%202019.11.20.pdf

Account Creation and Removal

- System IT staff should be notified of any personnel changes at a library that would require either the issuance of credentials to access PLS Systems (such as email or the ILS) or the termination of access to PLS Systems.
- Notifications of separations of service to PLS should occur immediately to ensure that individuals who should no longer have access to PLS Systems are removed as authorized users. Whenever possible, notification of separation of service should occur in advance of the date of separation.
- Library directors or their designees are responsible for informing Pioneer Library System of the separation from service of an individual who has/had access to a shared account (detailed below).
- A library's board president is responsible for informing Pioneer Library System of the separation from service of a library director.

Shared Accounts

- Shared accounts should be kept to a minimum and avoided whenever possible. When not able to be avoided, passwords shared between multiple authorized individuals shall be changed upon the separation from service of an individual no longer authorized to access PLS Systems. The responsibility to ensure that passwords are changed ultimately rests with the library director.
- Shared accounts include accounts that may be accessed by only one authorized individual at a time but which shall continue to be used after an individual's separation from service.
    - Any such accounts should also have their passwords changed upon a handover.
- Examples of appropriate shared accounts include:
    - A library's circulation email account.
    - An ad hoc email account created for a search committee.

Passwords

- Passwords used to access PLS Systems that contain patron PII shall be randomly generated[4], at least 12 characters long, unique, and should contain some level of complexity.
    - Examples of adequate passwords include:

[4] Use a password generator to create a password. Password generators are often offered by password managers, like the generators offered by 1Password (https://1password.com/password-generator/) or LastPass (https://www.lastpass.com/password-generator).

        - A "diceware" password[5] (a string of randomly generated dictionary words)
        - If using a "diceware" password, the password shall consist of a minimum of five randomly generated words.
        - A password that is at least 12 random characters long.
- Passwords shall not:
    - Consist of previously used passwords; or
    - Consist of passwords used for personal accounts.
- Passwords used to access PLS Systems shall not be transmitted in plain text (such as by email).
    - An exception can be made for passwords transmitted for one-time use, i.e. passwords used for an initial login that the recipient should then change after they are able to access the system.
- If an account or password is suspected to have been compromised, report the incident to System staff immediately by emailing support@pls-net.org.

Accessing PLS Systems

This portion of the policy establishes that both the electronic and physical security of devices used to access PLS Systems is important for maintaining the security of the network as a whole.

Electronic Security

- Only devices meeting all of the following requirements shall be used to access the ILS or the PLS reporting tool with staff credentials:
    - Device must be library-owned;
    - Device must be designated only for staff use (i.e., should not be lent to the public);
    - Device must have an up-to-date operating system;
    - Device must have up-to-date virus protection; and
    - Device must have an up-to-date web browser.
- No file containing patron PII should be downloaded to or stored on personal devices.
    - Such files include, but are not limited to:
        - files generated by the ILS;
        - files transmitted via email; or
        - files accessed on the PLS reporting tool.

Physical Security

[5] The EFF (Electronic Frontier Foundation) offers a guide to, and tool for, generating passwords by dice: https://www.eff.org/dice

- Devices on which patron PII is stored or accessed should be properly secured against unauthorized access.
- Devices should be locked or logged out of when not in use or when a staff user is not at (or within immediate line of sight of) the workstation.

Management of Files, Reports, and/or Documents Containing Patron PII

Best practices for handling files, reports, and/or documents containing patron PII include, but are not limited to:

- Accessing files or any links to files only on library-owned equipment and avoiding using personally-owned computers, mobile devices, and services, like Dropbox, to access, save, or store files.
- Making sure that files and printed copies are kept secure from unauthorized access.
- Avoiding transmitting files using methods that may not be secure, such as by email attachment. Instead, transmit files by using a shared drive on your local network or removable media like a flash drive.
- Avoiding sharing files with, or uploading files to, unauthorized third-parties or third-party services.
- Deleting files and emptying the recycling bin/trash when you are done with them.
- Shredding any printed copies when you are done with them.

<u>Handling PII</u>

This portion of the policy supplements the Pioneer Library System Confidentiality of Library Records Policy to establish what types of data about patrons should be stored in PLS Systems and how patron PII accessed in PLS Systems may be used.

Appropriate Collection of Data

- Only data necessary to provide library services should be stored in shared PLS Systems (like the ILS). The least amount of personally identifiable information possible should be collected and stored in PLS Systems.
- Data about patrons should only be stored in PLS Systems for the length of time necessary for operational or legal purposes.
    - Examples of data appropriate for collection include:
        - Name
        - Address
        - Email address
        - Telephone number
        - Date of birth

- Examples of data inappropriate for collection include:
  - Health information
  - Driver's license numbers

Appropriate Use of Data

- Patron PII should be used only for providing library services, such as for contacting patrons to inform them of available holds, overdue materials, etc.
- Any use of patron PII accessed from PLS Systems beyond providing library services must be a use for which a patron has explicitly consented to and opted-in.
- Patron PII should never be exported from any PLS Systems for the purpose of being shared with or uploaded to any third-party or third-party services.
  - Examples of third-parties include, but are not limited to, Friends groups and foundations.
  - Examples of third-party services include, but are not limited to, fundraising platforms, Dropbox, Google Drive.

Justification

NIST (National Institute of Standard and Technology): Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B)[6]

Q-B05: Is password expiration no longer recommended?[7]

A-B05:

SP 800-63B Section 5.1.1.2 paragraph 9 states:

"Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator."

Users tend to choose weaker memorized secrets when they know that they will have to change them in the near future. When those changes do occur, they often select a secret that is similar to their old memorized secret by applying a set of common transformations such as increasing a number in the password. This practice provides a false sense of security if any of the previous secrets has been compromised since attackers can apply these same common transformations. But if there is evidence that the memorized secret

[6] Digital Identity Guidelines, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
[7] NIST Special Publication 800-63: FAQ, Q-B05, https://pages.nist.gov/800-63-FAQ/#q-b05

has been compromised, such as by a breach of the verifier's hashed password database or observed fraudulent activity, subscribers should be required to change their memorized secrets. However, this event-based change should occur rarely, so that they are less motivated to choose a weak secret with the knowledge that it will only be used for a limited period of time.

Q-B06: Are password composition rules no longer recommended?[8]

A-B06:

SP 800-63B Section 5.1.1.2 paragraph 9 recommends against the use of composition rules (e.g., requiring lower-case, upper-case, digits, and/or special characters) for memorized secrets. These rules provide less benefit than might be expected because users tend to use predictable methods for satisfying these requirements when imposed (e.g., appending a ! to a memorized secret when required to use a special character). The frustration they often face may also cause them to focus on minimally satisfying the requirements rather than devising a memorable but complex secret. Instead, a blacklist of common passwords prevents subscribers from choosing very common values that would be particularly vulnerable, especially to an online attack.

Composition rules also inadvertently encourage people to use the same password across multiple systems since they often result in passwords that are difficult for people to memorize.

Q-B10: Does SP 800-63B require that we remove our password composition (complexity) rules?[9]

A-B10:

SP 800-63B Section 5.1.1.2 states in part:

Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets.

This text is a recommendation, not a normative requirement (i.e., "should" rather than "shall" in text). However, research has shown that composition rules do not significantly improve the security of selected passwords. Composition rules often have the opposite effect as users tend to avoid or shortcut the rules by making predictable changes, resulting in weaker passwords and less security. Instead, SP 800-63B requires the use of a blacklist

[8] NIST Special Publication 800-63: FAQ, Q-B06, https://pages.nist.gov/800-63-FAQ/#q-b06
[9] NIST Special Publication 800-63: FAQ, Q-B10,https://pages.nist.gov/800-63-FAQ/#q-b10

of common passwords that are not acceptable for use. We do recommend increased password length as a key password security control, especially through encouraging the use of passphrases.

NIST (National Institute of Standard and Technology): Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (SP 800-122)[10]

2.3 PII and Fair Information Practices

Purpose Specification—The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.

ALA Privacy and Confidentiality Q&A[11]

3. What is explicit consent and how is it different from opt-out? Explicit consent means that users are given an option to agree or disagree with the collection of their data. The user must be informed in a specific and unambiguous manner regarding how their data will be collected, used, and/or shared. Users should be given the choice before choosing to access a service rather than have to opt-out later. Libraries should ensure their online services do not default to opt-out. Opt-out requires action from the user to remove themselves from data collection. This does not allow a user to learn about the specific details of how their data will be utilized.

21. Can circulation or registration information be used for other library purposes, such as to generate mailing lists for fund-raising by the library or its Friends group? The Fair Information Practice Principles of "Notice and Openness" and "Choice and Consent" should be reflected in library privacy policies. See "How to Draft a Library Privacy Policy."

Some states impose restrictions on the use of personally identifiable information (PII) for any purposes other than circulation or administration. In other states it is illegal to provide library user PII to any third party except under court order. See "State Privacy Laws

---

[10] NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

[11] ALA, Privacy and Confidentiality Q&A, http://www.ala.org/advocacy/intfreedom/privacyconfidentialityqa

Regarding Library Records." In all states, regardless of the status of the law, library policies regarding the collection, use and dissemination of PII should be carefully formulated and administered to ensure that they do not conflict with the ALA Code of Ethics that states "we protect each user's right to privacy and confidentiality." Libraries choosing to use PII for any library-related purpose other than for which the PII was gathered should consider the following standard "opt-in" practices:

- *Notice should be provided to all users of any library use of PII.*
- *Any use of PII beyond circulation or administration should be authorized only on an opt-in basis. At the time of registration, users should be asked to opt-in to additional and specifically enumerated uses of their PII (e.g., for fund-raising appeals). The PII of those who decline to 'opt-in' should not be made available for any additional uses.*
- *Any time a library decides to extend use of PII in ways not already authorized, it must seek user opt-in. Libraries should presume that all non-responders wish to opt out of the new use.*

22. Does the library's responsibility for user privacy and confidentiality extend to licenses and agreements with outside vendors and contractors? Most libraries conduct business with a variety of vendors in order to provide access to electronic resources, to acquire and run their automated systems, to offer remote storage (e.g. "cloud computing), or to enable access to the internet. Libraries need to ensure that contracts and licenses reflect their policies and legal obligations concerning user privacy and confidentiality. Whenever a third party has access to personally identifiable information (PII), the agreements need to address appropriate restrictions on the use, aggregation, dissemination, and sale of that information, particularly information about minors. In circumstances in which there is a risk that PII may be disclosed, the library should warn its users and/or discontinue use of that service. In addition, all library vendors and contractors that handle PII should be expected to maintain a publicly available privacy policy that commits to compliance with the NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems.

NISO (National Information Standards Organization): NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems (NISO Privacy Principles)[12]

3. Security The most current security best practices should be used as the baseline to protect data. These should include encryption of personal data while they are at-rest and

[12] NISO Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems, https://groups.niso.org/apps/group_public/download.php/16064/NISO%20Privacy%20Principles.pdf

in-motion; prompt updates of systems and software to address vulnerabilities; systems, procedures, and policies for access control of sensitive data; a procedure for security training for those with access to data; and documented procedures for breach reporting, incident response, and system, software, and network security configuration and auditing.

Unauthorized access to user data should be remedied in a timely manner in order to minimize exposure of such data and affected parties should be informed as soon as is practicable in compliance with applicable laws. Libraries, content-, and software providers should comply with applicable statutory or regulatory requirements and published security standards intended to promote the privacy and security of user data.

4. Data Collection and Use The potential benefit to the user, the library, content-, or software-provider derived from the collection and use of users' personal data must be balanced against the impact of that collection and use on users and their right to privacy. Collection and use of users' personal data should be for the purposes of supporting user services, research to improve those services, or for the internal operations of the library, content-, or software-provider for which the data were gathered. The effective management and delivery of library services may require the library user to opt into the provision of personal data in order to access a library resource or receive library services. Users' personal data should only be used for purposes disclosed to them and to which they consent.

6. Options and Informed Consent Each library user's needs and expectations of privacy are different and may be contingent on circumstances. When personal data are not required to provide services as described in "Data Collection and Use", libraries and content- and software-providers should offer library users options as to how much personal information is collected from them and how it may be used. The default approach/setting should be that users are opted out of library services until they explicitly choose to opt in. In cases where a user opts in to a specific service, they should have the choice to opt out at a later date, in particular when privacy policies change, and at that time have the option to delete data as outlined in "Access to One's Own User Data" (item 10 below).

7. Sharing Data with Others Libraries, content-, and software-providers sometimes need to share some data to provide content or library services, or undertake administrative functions. However, these parties must carefully consider the impact on the user's privacy before sharing data or information about their activity with third parties. Such considerations should include: the library user's consent; the user's privacy interests; any legal prohibitions or requirements; the policies of that third party and their adherence to these principles; and the risks and benefits to the user and institution.

User activity data to be shared should be anonymized and aggregated to a level that minimizes privacy risks to individual users, unless the user has opted-in to a service. In particular, possible exposure of the resource-use habits of individual users should be protected in conformance with the "Anonymization" principle (item 5 above).

Adopted: Date