2016-2017 ALA CD #19.1 Report from the Intellectual Freedom Committee
2017 ALA Midwinter Meeting

Library Privacy Checklist
Overview

This is checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines. It is an overview checklist that highlights general actions that are applicable across multiple guidelines. There are also specific checklists that libraries can consult for each guideline.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions
Create a policy that addresses the collection of patron information. Such a policy should specify that the library is not collecting more patron information than what it needs and that it is not keeping the personally identifiable information of patrons longer than what is necessary.
Create a privacy policy that is understandable by a layperson.
Make sure the privacy policy is posted in the library where the public can see it.
Ensure that the privacy policy includes information about what information the library is tracking, why, and for how long the data is kept.
Ensure that the privacy policy includes when patron information can be shared and under what conditions.
Destroy all paper records with user data, such as computer sign-in sheets.
Ensure all existing security certificates for HTTPS/SSL are valid and create a procedure for revalidating them annually.
Designate a Library Privacy Officer to handle requests for personally identifiable information of patrons from law enforcement officials and other third parties.

Priority 2 Actions
Ensure there is a formal process in place to address breaches of patron data directly under library control or maintained by third parties. The library should notify affected users when they become aware of a breach.
Encrypt all user data with secure algorithms in all network and application communications.
Purge search history records regularly, ideally when the individual computer session ends.
Purge circulation and interlibrary loan records when they are no longer needed for library operations. Any patron data that is kept for analysis should be anonymized or de- identified and have access restricted to authorized staff.
Utilize HTTPS wherever possible.
Ensure that the privacy policy is updated often and schedule regular times for its review.

Priority 3 Actions
Publish and distribute flyers and/or web content for patrons that includes information on how to protect personally identifiable information and other data.

Publish and distribute flyers and/or web content for patrons about available software and alternative browsers and plugins to protect their privacy online and can be used in the library.
Publish and distribute flyers and/or web content about VPN services and/or Tor and patrons' ability to use these systems on the library network.
Test compliance with these standards through a trusted third party service or individual.

Resources

ALA's Guidelines for Developing a Library Privacy Policy: http://www.ala.org/advocacy/privacyconfidentiality/guidelines-developing-library-privacy- policy
How to Geek's 5 Alternative Search Engine's That Respect Your Privacy: http://www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your- privacy/
ALA's Library Bill of Rights: http://www.ala.org/advocacy/intfreedom/librarybill
ALA's Privacy Toolkit: http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy
EFF Surveillance Self Defence - Choosing the VPN That's Right for You: https://ssd.eff.org/en/module/choosing-vpn-thats-right-you
EFF Surveillance Self Defence - Introduction to Threat Modeling: https://ssd.eff.org/en/module/introduction-threat-modeling
EFF Surveillance Self Defence - Keeping your Data Safe: https://ssd.eff.org/en/module/keeping-your-data-safe
EFF Surveillance Self Defence - Seven Steps to Digital Security: https://ssd.eff.org/en/module/seven-steps-digital-security
NIST'S Policy on Hash Functions http://csrc.nist.gov/groups/ST/hash/policy.html

2016-2017 ALA CD #19.2
2017 ALA Midwinter Meeting

Library Privacy Checklist
for
Library Websites, OPACs, and Discovery Services

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Library Websites, OPACs, and Discovery Services.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions
Establish a library privacy policy which includes data privacy and security policies based on legal regulations and professional/industry standards.
Ensure that the privacy policy is readily available in easy-to-understand language to users of a library website, social media site, OPAC or discovery service.
Provide links to third party privacy and terms of service pages for users when appropriate.
Limit the amount of personal information collected about users. In general, the library or service provider should collect the minimum personal information required to provide a service or meet a specific operational need.
Provide users with options as to how much information is collected from them and how it may be used. Users should have a choice about whether or not to opt-in to features and services that require the collection of personal information such as borrower history, reading lists, or favorite books.
Configure services directly under library control to use the opt-in method whenever possible for features that involve the collection of personal information.
Work with providers to configure external services to use the opt-in method whenever possible for features that involve the collection of personal information. This ability to opt-in should be an important criteria when the library decides to select or renew a service.
Users should also have the ability to opt-out if they later change their minds and have the data collected during the opt-in phase be destroyed when possible.
Establish procedures that restrict access to personal information to the user or appropriate library staff and conform to the applicable state laws addressing the confidentiality of library records as well as other applicable local, state, and federal law. Ideally these procedures are supported by technical measures such as role-based permissions for staff account.
Provide training to library staff who manage the library's websites, OPACs, and discovery services on the library's privacy policy and best practices for safeguarding patron privacy. Library staff that negotiate contracts with vendors that provide websites and services should also receive privacy training.

Priority 2 Actions
Create a proactive process to notify ongoing users of any changes to the library's privacy policy or any violations in user privacy through inadvertent dissemination or data theft.

In the event of a data breach libraries should describe what steps are being taken to remedy the situation or mitigate the possible damage, and what steps patrons should take to protect themselves.
Consider enacting canary warnings to notify patrons when information may have been subpoenaed through a court order.
Evaluate the impact on user privacy of all third-party scripts and embedded content (e.g. cover images, ratings, reviews, etc.) that are included in a library website, OPAC, or discovery service.
Limit use of Javascripts from third-parties on library sites.
Avoid Flash-based plugins.
Review any terms of service for scripts and embedded content, as they often allow the third party to harvest user activity data for their own purposes.
Consider alternative solutions that better respect user privacy. For example, use Piwik for web analytics instead of Google Analytics.
Do not retain in perpetuity any user activity data with personally identifiable information.
Establish policies for how long to retain different types of data and methods for securely destroying data that is no longer needed.
Retention policies should also cover archival copies and backups.
Anonymize or de-identify user data stored for assessment or metrics. Anonymization provides better protection than de-identification.
Anonymize reports and web analytics intended for wider distribution by removing or encrypting personally identifiable information.
Provide users the ability to access their own personal information and evaluate its accuracy.
Guidance on how the user can access their personal data and offer corrections if needed should be clear and easy to find.
Ensure that all services directly under library control are secure.
Stay aware of and remediate known exploits.
Keep software and applications up-to-date.
Monitor logs for intrusions and perform regular security audits.
Perform regular backups and have a disaster recovery plan. Note that backups should be subject to your policy on data retention.
Work with service providers to review contracts/licenses and if needed revise them so that they are in compliance with relevant legal regulations and library policy.
Create an addendum to contracts regarding liability for data breaches that affect user privacy.

Priority 3 Actions
Establish and maintain effective mechanisms to enforce library privacy policies. Conduct regular privacy audits to ensure that all operations and services comply with these policies.
Encrypt all online transactions between client applications (web browsers, e-book readers, mobile apps, etc.) and server applications using modern, up-to-date security protocols for SSL/HTTPS. Communications between server applications and third-party service providers should be encrypted.
Store user passwords using up-to-date best practices for encryption with a cryptographically secure hash.
Ensure that any personally identifiable information and user data housed off site (cloud- based infrastructure, tape backups, etc.) uses encrypted storage.
Explore the possibility of two-factor authentication and implement if possible.

Resources

Example Privacy Policy from NYPL
Personally Identifiable Information
HTTPS Everywhere
Let's Encrypt
How to Check if your Library is Leaking Catalog Searches to Amazon
Warrant Canary
A Visual Guide to Practical Data De-Identification
NISTIR 8053: De-Identification of Personal Information
Password Storage Cheatsheet

2016-2017 ALA CD #19.3
2017 ALA Midwinter Meeting

Library Privacy Checklist for Students in K-12 Schools

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Students in K-12 Schools.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions
Create internal library procedures to protect student privacy based on:
school policies related to privacy and confidentiality of student data, especially student circulation records and the use of library resources in all formats.
federal laws such as the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), and state privacy laws regarding library records.
ALA and AASL policy statements, online tool kits and Q&As, guidelines, and other resources provided by national and state library associations.
Collect the minimum amount of information necessary about students to conduct library business.
Configure circulation software to delete students' borrowing history and retain only necessary records.
Ensure any paper records with sensitive information are stored in a secure area and shredded when no longer needed.
Train library staff and volunteers to respect students' privacy and the confidentiality of their library records.

Priority 2 Actions
Educate administrators, faculty, and support staff about students' library privacy and the confidentiality of student data using a variety of communication methods.
Initiate conversations with the principal, teachers, students, and parents about the need for an official library privacy policy.
Add privacy-related resources to the library collection including items related to personal privacy, minors' privacy rights, and privacy as a national and international issue.
Consider creating a privacy information section on the school library web page or a privacy-themed pathfinder (e.g. LibGuide) with privacy resources.
Integrate online privacy into library instruction and programming. For example:
Introduce students to online privacy information such as secure passwords and web tracking during library orientations and other brief presentations.
Celebrate Choose Privacy Week and other privacy-related observances (Data Privacy Day, Teen Tech Week, etc.) with the school community.
Create privacy-related displays and set up videos in the library to educate parents during parent-teacher conferences and other evening school and community events
Offer presentations to parents about students' privacy online and other topics of interest to families.

Advocate within the school or district for protecting students' privacy rights in learning management systems or other technologies that enable educators to monitor student reading and research habits. Assessment should not include monitoring how students use specific library materials and online resources as part of free inquiry and research.
Volunteer to serve on the school's data governance committee. If one does not exist, advocate for its creation.

Priority 3 Actions
Work with other stakeholders in the school or district to create an official library privacy policy in regards to student circulation records and the use of library resources.
The privacy policy should be approved by the school's governing body (e.g. school board, school committee, etc.)
Post the policy in the library and on the library's section of the school website.
Promote the library's privacy policy within the school community.
Work through school lines of authority to write or adapt a K-12 privacy curriculum and have it formally approved and taught. Collaboratively teach privacy units with teachers using the iKEEPSAFE and/or other privacy curricula.
Work with school officials to incorporate privacy protections into RFP's and resulting contracts.
Discuss privacy concerns with digital resource and technology vendors, especially in regards to the school's/library's contracts with these vendors.
Ensure that all online transactions between client applications and server applications are encrypted.
Ensure that storage of personally identifiable student information is housed using encrypted storage.

Resources

ALA/AASL Policy Statements

ALA/AASL Policy Statements Position Statement on the Confidentiality of Library Records. http://www.ala.org/aasl/advocacy/resources/statements/library-records
ALA. 2008. Code of Ethics. http://www.ala.org/advocacy/proethics/codeofethics/codeethics
ALA. 2014. Privacy: An Interpretation of the Library Bill of Rights. http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Legislation

American Library Association. State Privacy Laws Regarding Library Records. http://www.ala.org/advocacy/privacyconfidentiality/privacy/stateprivacy
Federal Trade Commission. Children's Online Protection Act (COPPA) Rule. https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform- proceedings/childrens-online-privacy-protection-rule
U.S. Department of Education. Laws and Guidance: Family Educational Rights and Privacy Act (FERPA). http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
U.S. Department of Education. Laws and Guidance: Family Policy Compliance Office. http://www2.ed.gov/policy/gen/guid/fpco/index.html

Learning Resources

ALA. Choose Privacy Week. Students and Minors' Privacy- Selected Resources. https://chooseprivacyweek.org/students-and-minors-privacy/
ALA. Intellectual Freedom News. Note: Subscribe to future issues of Intellectual Freedom News, a free biweekly compilation of news delivered via email by the ALA Office for Intellectual Freedom. Web form URL: http://ala.informz.net/ala/profile.asp?fid=3430
ALA. 2014. Privacy Tool Kit. http://www.ala.org/advocacy/privacyconfidentiality/toolkitsprivacy/privacy
ALA. 2014. Questions and Answers on Privacy and Confidentiality. http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/qa-privacy
Christine Eldred. Colchester High School (VT) Intellectual Freedom LibGuide. (with Choose Privacy Week tab) http://chs.csdvt.libguides.com/intellectualfreedom
Common Sense Media. Privacy and Internet Safety [Information aimed at parents]. https://www.commonsensemedia.org/privacy-and-internet-safety#
Consortium for School Networking. Protecting Privacy in a Connected World. http://cosn.org/focus-areas/leadership-vision/protecting-privacy
Library Freedom Project. "Teen Privacy Guide." https://libraryfreedomproject.org/teenprivacyguide/
National Cyber Security Alliance. "Privacy Library." https://staysafeonline.org
YALSA. Teen Tech Week. http://teentechweek.ning.com/page/faq
U.S. Department of Education. Privacy Technical Assistance Center. http://ptac.ed.gov/

Teaching Tools

ALA. Choose Privacy Week Programming Guide and Activities. 2010 http://chooseprivacyweek.org/wp- content/uploads/2013/04/CPWResourceGuideProgram.pdf
iKEEPSAFE. K-12 Curriculum Matrix. November 2015. http://ikeepsafe.org/privacy-k-12-curriculum-matrix/
San Jose Public Library. Virtual Privacy Lab. (modules in English, Spanish, and Vietnamese) https://www.sjpl.org/privacy

Digital Defenders (free, CC-licensed kids' booklet about privacy) https://edri.org/files/privacy4kids_booklet_web.pdf

Advocacy

Data Quality Campaign and Consortium for School Networking. Student Data Principles. http://studentdataprinciples.org/the-principles/

Electronic Privacy Information Center. Student Privacy Bill of Rights. https://epic.org/privacy/student/bill-of-rights.html

Future of Privacy Forum (FPF) and the Software and Information Industry Association (SIIA). Student Privacy Pledge. https://studentprivacypledge.org/privacy-pledge/

2016-2017 ALA CD #19.4
2017 ALA Midwinter Meeting

Library Privacy Checklist
Public Access Computers and Networks

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Public Access Computers and Networks.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions
Use analog signage and/or splash screens to explain the library's network and Wi-Fi access policies, including any privacy-related information.
Make a policy decision about the level of privacy versus convenience that the library will offer its Wi-Fi users and adequately warn users of potentials for traffic interception and other risks of an insecure network.
Set up public computers to purge downloads, saved files, browsing history, and other data from individual user sessions. This can be accomplished
on logout via the computer reservation system if the library uses such a system;
by using restoration software such as CleanSlate or Deep Freeze;
by configuring browsers to clear all history and other usage data upon exit.
Ensure that paper sign-up sheets for public computers, devices, or classes are destroyed when no longer needed.
Offer classes and other educational materials to users about best practices for privacy and security when using the library's public computers.
Offer privacy screens to patrons who desire to use them.

Priority 2 Actions
Use antivirus software on all public computers. Ensure that antivirus software that is installed has the ability to block spyware and keylogging software.
Ensure that any computer reservation management system records, print management records, or ILS records in regards to computer use are anonymized or destroyed when no longer needed.
Configure any content filters to not collect or store browsing data.
Anonymize or destroy transactional logs for network activity when no longer needed.

Perform regular security audits on all public computers, including digital inspection of security risks and flaws and physical inspection for unknown devices.

Priority 3 Actions
Install plugins on public computers to limit third party tracking, enable private browsing modes, and force HTTPS connections.
HTTPS Everywhere: https://www.eff.org/https-everywhere
Privacy Badger: https://www.eff.org/privacybadger
See guides about Firefox security options, e.g. https://securityinabox.org/en/guide/firefox/windows
Install the Tor browser on public computers as a privacy option for patrons.
Offer the privacy-oriented Tails OS on bootable USB or CDROM for use on public computers or patron devices.
Install malware-blocking, ad blocking, and anti-spam features on firewalls.
Segment the network to isolate staff computers, public computers, and wireless users into their own subnets.
Ensure that any applications and operating systems on public computers are disabled from automatically sharing activity data with software publishers (e.g. error reporting).

Resources:

https://securityinabox.org/en/guide/basic-security/windows

https://libraryfreedomproject.org/resources/privacytoolkit/

http://www.dataprivacyproject.org/mapping-data-flows/

https://www.consumer.ftc.gov/media/video-0080-public-wi-fi-networks

https://www.sjpl.org/privacy/security-how-internet-works

https://www.f-secure.com/en/web/labs_global/threat-descriptions

http://www.howtogeek.com/221929/how-to-choose-the-best-vpn-service-for-your-needs/

http://www.niso.org/apps/group_public/download.php/16064/NISO%20Privacy%20Principles.pdf

https://www.amazon.com/Protecting-Patron-Privacy-Practices-Computers/dp/1610699963

2016-2017 ALA CD #19.5
2017 ALA Midwinter Meeting

Library Privacy Checklist
For E-book Lending and Digital Content Vendors

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for E-book Lending and Digital Content Vendors.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions
Provide links to vendor privacy policies and terms of service pages for users when appropriate, e.g. from the library's own privacy policy page or from a library web page about the vendor's product or service.
Work with vendors to configure services to use the opt-in method whenever possible for features that involve the collection of personal information.
Develop a strategy to assist patrons in managing their privacy when using vendor products and services. The strategy could include in-person reference, handouts, web guides, classes, or other programming. Topics covered could include:
Settings for personal accounts on vendor websites.
Vendor applications on personal devices including any privacy settings and how to remove the application and any associated stored data.
Notify staff and patrons of any data breaches and assist patrons in mitigating the impact (changing passwords, uninstalling applications, etc.).

Priority 2 Actions
Add privacy considerations to the library's selection criteria for new purchases or the renewal of existing purchases. These considerations should include the vendor:
Notifying users of their privacy policies at the point of access and restricting the collection of patron data to clearly stated operational purposes.
Seeking patron consent for data collection by using the opt-in method whenever possible for features that involve the collection of personal information.
Providing a method for patrons to access, review, correct and delete their personal data.
Encrypting connections using SSL/HTTPS to provide secure access to digital content.
Allowing users to uninstall vendor applications and delete associated stored data from personal devices.
Review all new license agreements regarding the use, aggregation, retention, security, and dissemination of patron data. Before purchasing a new product or service the library should ensure that the license agreement:
Complies with all applicable local, state, and federal laws regarding the confidentiality of library records.
Conforms to the library's privacy, data retention, and data security policies.
Stipulates that the library retains ownership of all patron data.
Includes a protocol for responding to government and law enforcement requests for patron data.

States the vendor's responsibilities to notify the library and affected patrons in the event of a data breach.

Priority 3 Actions
Review existing license agreements using the privacy concerns outlined above for new agreements.
Work with vendors to change language of license agreements when possible to address concerns.
Consider not renewing contracts with vendors that are unable to provide these assurances in the license agreement.
Review vendors' data governance plan that addresses patron consent, data security, encryption, anonymization, retention, dissemination/data sharing, and destruction. If the vendor does not have a plan, ask them to create one.
Request that vendors conduct regular privacy audits and make audit results available to the library for review. Make the results of the review one of the criteria for renewal.

Resources

ALA. "Encryption and Patron Privacy." American Library Association, 2016, www.ala.org/advocacy/encryption-and-patron-privacy
Cavoukian, Ann. "Privacy by Design: The 7 Foundational Principles; Implementation and Mapping of Fair Information Practices." Internet Architecture Board, 2011, https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
Department of Computer Engineering, Boğaziçi University. "Guide to Data Protection Auditing." Data Protection, http://www.cmpe.boun.edu.tr/~ozturan/etm555/dataaudit/html/refer/checks/index.htm
Hoffman-Andrews, Jacob. "What Every Librarian Needs To Know About HTTPS." Electronic Frontier Foundation, 6 May 2015, https://www.eff.org/deeplinks/2015/05/what-every-librarian-needs-know-about-https
International Association of Privacy Professionals. "Security Breach Response Plan Toolkit." IAPP Resource Center, 2016, https://iapp.org/resources/article/security-breach-response-plan-toolkit/
Internet Security Research Group. Let's Encrypt [https certificate registry], https://letsencrypt.org/

Perera, Charith, McCormick, Ciaran, Bandara, Arosha K., Price, Blaine A., and Bashar Nuseibeh. "Privacy-By-Design Framework for Assessing Internet of Things Applications and Platforms." IoT 2016, 7-9 Nov. 2016, Stuttgart, Germany, https://arxiv.org/pdf/1609.04060v1.pdf
Riffat, Muzamil. "Privacy Audit - Methodology and Related Considerations." ISACA Journal, vol. 1, 2014, http://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Privacy-Audit-Methodology-and-Related-Considerations.aspx
Chmara, T. (2012). Privacy and E-Books. Knowledge Quest, 40(3), 62-65.

Additional Questions to Consider

What are the local statutes regarding patron/user information use?

Does the vendor's privacy policy jive with the library's privacy policy?

Is the vendor's privacy policy explicit on the product portal?

Can the vendor's privacy policy be shared with the library to publicize for its users?

User's browsing, borrowing, downloads, notations, group affiliations shall not be shared with any other parties without the specific written consent of the individual user.
Does the language in the policy/contract/license specifically address other devices and do the terms extend to other devices as well (smartphone apps, tablet, etc.)?
What is the retention policy of the institution/library, including proxy server collection of IP address access, and what is the retention policy of the vendor?
Is the language of the policy consistent with the age of the product's intended audience, can the minor user for instance understand the policy?
Does the language of the policy/contract/license specify that harvested user data should be destroyed and not retained in perpetuity by the vendor?
In case of data breach, does the language specify that the vendor inform the library as soon as it is aware of the breach?
How should the library respond in terms of user privacy when a data breach is identified?
Vendor must give libraries advance notice of any changes to the user privacy policies, at least 30 days to respond.
Agreements and contracts should be reviewed annually per their individual renewal/ purchase date.

2016-2017 ALA CD #19.6
2017 ALA Midwinter Meeting

Library Privacy Checklist for Data Exchange Between Networked Devices and Services

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Data Exchange Between Networked Devices and Services.

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions
Establish minimum security practices for devices and services.
Change any default passwords.
Disable remote access to the superuser account (i.e. root or administrator).
Keep all software up-to-date using a secure and verified source.
Require authentication for all client connections to services that allow access to patron information.
Limit clients to only the access they need, i.e. the least privilege model.
Enable mutual authentication of server and client if supported.
Use a secure authentication standard such as oauth when feasible.
Implement a logging policy for devices and services that covers rotation and retention, types of data collected, and the implications on patron privacy.

Priority 2 Actions
Harden security on devices and services.
Disable any extraneous services that are running on devices.
Limit administrative privileges to authorized individuals through user access controls or the sudo program.
Require a unique password for each instance of a service.
Implement and enforce a strong password policy that specifies password length, formation, and duration. Consider using randomly generated passwords.
Encrypt data communications between client applications and server applications that may include patron information.
Configure services when possible to require encryption by default, i.e. do not allow unencrypted connections.
If services do not support encryption (e.g. SIP2), use an encrypted transport such as SSH tunnel or a VPN.
Encrypt sensitive data at rest (i.e. data warehouses, archives, tapes, offsite backups, etc.).
Store passwords in applications using up-to-date best practices for encryption (i.e. hashed and salted).
Priority 3 Actions
All remote access (including SSH) should be through secure keys not passwords.
Keys should be no less than 2048 bit, 4096 bit is preferable.
Do not allow deprecated or insecure ciphers.
Ensure private keys are secure (use subkeys and keep master keys very safe).
Rotate keys regularly and be ready to revoke them in case of compromise.

Review the protocols employed by devices and services. Protocols should:
Be standard, established, and open.
Not be deprecated due to security concerns.
Support data integrity including origin authentication, non-repudiation of origin, non-repudiation of receipt, and verification of payload using cryptographic signature or a hash.
Verify security of devices and services by using penetration testing tools.

Resources
Passwords: CPNI

Burr, W. E., Dodson, D. F., & Elaine, M. (2011). Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus. Electronic authentication guideline. NIST Special Publication, 800-63.
Chandramouli, R., Iorga, M., & Chokhani, S. (2014). Cryptographic key management issues and challenges in cloud services. In Secure Cloud Computing (pp. 1-30). Springer New York.
Hoeper, K. & Chen, L. (2009). Recommendation for EAP Methods Used in Wireless Network Access Authentication. Retrieved from: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-120.pdf
Jakimoski, K. (2016). Security Techniques for Data Protection in Cloud Computing. International Journal of Grid and Distributed Computing, 9(1), 49-56.
Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800(144), 10-11.
National Center for Education Statistics (Ed.). (n.d.). Chapter 6: Maintaining a Secure Environment, Weaving a Secure Web around Education: A Guide to Technology Standards and Security. Retrieved from https://nces.ed.gov/pubs2003/secureweb/ch_6.asp
Peng, C., Kesarinath, G., Brinks, T., Young, J., & Groves, D. (2009). Assuring the Privacy and Security of Transmitting Sensitive Electronic Health Information. AMIA Annual Symposium Proceedings, 2009, 516–520.
Singhal, A., Winograd, T., & Scarfone, K. (2007). Guide to secure web services. NIST Special Publication, 800(95), 4.
Tysowski, P. (2016). OAuth Standard for User Authorization of Cloud Services. Encyclopedia of Cloud Computing, 406-416

2016-2017 ALA CD #19.7
2017 ALA Midwinter Meeting

Library Privacy Checklist for Library Management Systems / Integrated Library Systems

This checklist is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the Library Privacy Guidelines for Library Management Systems. Library Management Systems (LMS) are also known as Integrated Library Systems (ILS).

Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

Priority 1 Actions
Develop a privacy policy about patron information in the LMS and publish it on the library's website in a place that is easy to find.
Request and store only the personal information about patrons necessary for library operations.
Periodically remove data that is no longer necessary for library operations (e.g. purchase-request data).
If the LMS supports it, use "fuzz" demographic information wherever possible (e.g. use a "minor/ not a minor" classification instead of recording full birth date).
Aggregate or anonymize reports to remove personally identifiable information. Reports should be periodically reviewed to ensure they are not revealing this type of information.
Configure the LMS by default to remove transactional data between patrons and materials they borrow / access when it is no longer needed for library operations.
Allow patrons the ability to opt-in to personalization features like keeping their checkout history or a list of favorite titles.
Allow patrons to later opt-out of features if they change their mind. Ensure that data previously retained for these features is deleted when patrons opt out.
Develop procedures for library staff on how to handle law enforcement and government requests for patron records.

Priority 2 Actions
Restrict access to patron records in the LMS to staff members with a demonstrated need for it. For example, circulation staff need access but shelvers do not.
Configure library notifications for holds, overdues, etc. to send a minimal amount of personal information.
Develop policies and procedures regarding the extraction, storage, and sharing of patron data from the LMS for in-house or contracted third-party use.
Restrict access to the extracts to appropriate staff.
The policy should include disposal/deletion of extracts.
Encrypt offline data backups to prevent access by unauthorized personnel.
Keep LMS applications and underlying server software up-to-date to mitigate the impact of security vulnerabilities.

Priority 3 Actions
Store all passwords (patron and staff) in a secure fashion using a proper cryptographic hash function. At this time bcrypt or better are good standards.

Encrypt all traffic between the LMS server and any client connections outside a secure LAN. For example, use a VPN to encrypt the connection over the Internet of a checkout station at a branch library to the LMS server at the main library.
Conduct regular audits of the network and LMS servers to make sure reasonable security measures are in place to prevent unauthorized access.
Create procedures to handle data breaches to unauthorized parties and mitigate their impact on patrons.

Resources

Marshall Breeding's article from the January 2015 Smart Libraries Newsletter “Privacy and Security of Automation and Discovery Products” https://librarytechnology.org/repository/item.pl?id=20425
Electronic Privacy Information Center (EPIC)
The Code of Fair Information Practices https://epic.org/privacy/consumer/code_fair_info.html
Marshall Breeding - “Privacy and Security for Library Systems” Library Technology Reports [May/June 2016] https://librarytechnology.org/repository/item.pl?id=2167