Library Freedom Project / Vendor Privacy Audit

YOUR LIBRARY'S NAME

VENDOR

TODAY'S DATE

PRODUCT/DATABASE/TOOL

See the attached Infosheet for instructions on interpreting the questions below. Mark the applicable column for yes, otherwise leave blank.	GOOD	RISKY
Does the vendor have a privacy policy or Terms of Service with a privacy statement that is clear and easy to understand?		
Does the vendor track users?		
Does the vendor share patron data with 3rd parties?		
If the vendor collects patron data, do they collect only what is necessary to provide their specific service?		
If the vendor collects patron data, do they have clear retention and deletion procedures, preferably outlined in their privacy statement?		
If the vendor collects patron data, do they have clear procedures if a data breach occurs and are those procedures outlined in their privacy statement?		
Is the patron data encrypted at rest and in transit?		
Does the vendor delete data at the end of the business relationship?		
Does the vendor disallow anonymous use?		
Does the vendor regularly perform security audits?		
TOTAL Subtract the total of Column B from Column A for your Vendor's score.		

How to Interpret the Questions

1. It is important that the average library worker and/or patron be able to understand the vendor's privacy policy and/or Terms of Service. If the language uses high-level tech speak, check the Risky box. If the language is vague and uses terms like "reasonable" or fails to define terms for "user," "data," etc., check the Risky box. If the Terms of Service or the privacy policy cannot be found, check the Risky box.

2. Does the vendor track patrons by utilizing "click tracking" or "cookies" to track patrons' preferences and activities? Does the vendor use companies such as Google Analytics to collect statistical information about what web pages were visited, for how long, and how they were located? Libraries will need to balance the need for reliable metrics against patron privacy. Check the Risky box if the vendor uses "cookies" with no ability for the library or the patron to disable or severely limit them. Check the Risky box if the vendor uses Google Analytics (or some other click-tracking service) with no ability for the library to disable this.

3. Many vendors use 3rd parties to glean metrics from patron data for their own business purposes. Check the Risky box if the vendor shares patron data with 3rd parties.

4. The vendor should not collect non-essential data, meaning they should only collect what is necessary to provide their service. Check the Good box if the vendor only collects data that is absolutely necessary to provide you with their service. Check the Good box if the vendor collects non-essential but this is turned off by default, and the patron can turn this collection on and off at any time.

5. The vendor should be clear about how they safely store data and for how long. They should also state how they safely delete data. Check the Good box if the vendor clearly states their retention and deletion procedures. Check the Good box again if the library can change the data retention settings. (Up to two checks total.)

6. Many companies experience data breaches. Though we don't want this to happen, if it does, all vendors should be prepared to act quickly. Check the Good box if the vendor has clear security breach protocols that align with industry standards such PCI or NISO standards.

7. Data encryption, or data that is protected with encoding, is a very simple step that vendors can take in order to ensure patron privacy. There are two types of data that need to be encrypted: 1) Data "at rest", which is data that is stored on hard drives or other media; and, 2) Data "in transit," which is data that is en route to other computers. Check the Good box if the vendor encrypts both data at rest and data in transit.

8. Patron data must be deleted by the vendor when the business relationship ends. Check the Good box if the vendor commits to deleting patrons' data when the business relationship ends.

9. The vendor should support anonymous use if at all possible. In most cases, it is necessary for the vendor to collect patron data in order to provide the service. In these cases, the patron should be notified that anonymous use is not possible. Check the Risky box if the vendor requires patrons to sign in with no explanation that anonymous use is not possible. Check the Risky box again if the vendor requires patrons to sign in unnecessarily, meaning there is no need to collect the patron's data in order to provide the service.

10. Security audits help vendors assess their overall security structure by measuring how well their security protocols conform to established criteria. Check the Good box if the vendor performs security audits. Check the Good again if the vendor is willing to share some or all of the results from their most recent security audit. (Up to two checks total.)

How to Interpret the Results

Good Privacy Practices (Green) | 7-8 points: This vendor has good privacy practices that are in line with industry standards. It's important to continue to monitor all vendors, even those with good privacy practices, since all companies change over time.

Questionable Privacy Practices (Yellow) | 5-7 points: If you are already using this vendor, review their privacy statement and/or Terms of Service, and draw up a list of privacy changes you would like them to make in order for you to renew your contract. If you renew, continue to monitor them closely by performing regular audits. If you are not yet using this vendor, draw up privacy requirements you would like added to the contract. You will likely need to speak with your library's legal department to help draft the language.

Risky Privacy Practices (Red) | 4 points: Beware. This vendor engages in risky privacy practices. If you are already using this vendor, research its competitors and begin pursuing alternatives. Speak to your account representative, list out your concerns, and ask whether they would be willing to make the necessary changes to be in line with industry standards. If not, consider not renewing your contract. If you are not yet using this vendor, research their competitors to see if the alternative(s) have better privacy practices.

References

• Pacific Library Partnership Data Privacy Best Practices Toolkit for Libraries
https://www.plpinfo.org/dataprivacytoolkit

• Measuring Library Vendor Security: Seven Easy Questions Every Librarian Can Ask
https://journal.code4lib.org/articles/11413

• Library Freedom Vendor Privacy Scorecard
https://github.com/alisonLFP/libraryfreedominstitute/blob/master/LFI2/finalprojects/Library%20Freedom-%20Vendor%20Scorecard-%20110719.pdf

• How to Assess a Vendor's Data Security:
https://www.eff.org/deeplinks/2018/01/how-assess-vendors-data-security

• Protecting Patron Privacy: Vendors, Libraries, and Patrons Each Have a Role to Play:
https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1330&context=collaborativelibrarianship