UNDERSTANDING CONFIDENTIALITY AND RISK ASSESSMENT

A REFERENCE GUIDE FOR EVERYONE, EVERYWHERE

BY LAYLA MAURER, ESQ.

LIBRARY FUTURES

Understanding Confidentiality and Risk Assessment

A Reference Guide for Everyone, Everywhere

LAYLA MAURER

LIBRARY FUTURES
NEW YORK, NY

Contents

Introduction

About This Guide

Understanding Confidentiality and Risk Assessment: A Reference Guide for Everyone, Everywhere was developed by Library Futures Staff Attorney Layla Maurer as part of Library Futures's work supporting libraries in contract negotiations. The resources herein are meant to help librarians understand confidentiality and risk in order to empower them to read, understand, and negotiate library-vendor contracts. Nothing within this guide constitutes legal advice. Specific questions should always be addressed to qualified counsel.

About Library Futures

Library Futures is the vanguard nonprofit organization uncovering and confronting the fundamental policy issues that threaten libraries in the digital age. We believe librarians, policymakers, and community leaders deserve a new approach to digital rights so they can protect, advocate for, and advance a fair digital future for libraries and the communities they serve. Library Futures meets this need with fresh research, visionary policy and advocacy initiatives, and engaging education programs.

Library Futures is a project of the Engelberg Center on Innovation Law & Policy at New York University School of Law.

Visit us online.

Understanding Confidentiality

Last Updated: March 31, 2026

> ***Disclaimer: This guide provides a framework for analysis and is not legal advice. For specific ambiguities or high-stakes situations, refer to the Risk Assessment Guide or consult qualified legal counsel.***

"Confidentiality" rules in agreements protect certain types of information. How can you identify what type of information is protected, and what type of information can be freely shared??

The answer lies in ***shifting your mindset***. Start by asking the basic question: **"What can I share?"** — this will help you identify what information is actually considered "confidential."

Quick Start

Use this framework to analyze potential confidentiality obligations. (Often you'll find that you aren't as limited as you think!)

1. **Determine Your Obligations:** Confirm whether, and how, you're legally bound to silence.
2. **Analyze the Contract:** Locate the definition of "Confidential Information," any language inferring confidentiality, and any exceptions.
3. **Categorize the Data:** Use the steps outlined in this guide to filter the specific information you want to share.
4. **Move to Next Steps:** Know when to ask for help or how to assess risk.

Step 1: Determine Your Obligations

Before analyzing what you can say, first confirm whether you have any obligation to keep information confidential.

You Might Have a Legal Obligation of Confidentiality If:

- **You Signed Something:** Someone at your organization signed a Non-Disclosure Agreement ("NDA") or other agreement.
- **You Clicked Something:** Someone at your organization accepted a clickthrough "Terms of Service" or "EULA" before accessing software or a platform. ***NOTE: If your organization is using software, it's highly likely that someone agreed to that software's terms.***

You Likely Do NOT Have an Obligation If:

- **You Received Unilateral Notice:** You only received an email footer or verbal warning mentioning confidentiality, but never signed or agreed to anything.
- **There's No Contract:** Your organization has been in discussions with another party about business ideas or received a pitch, but hasn't signed any documents or started using that party's software or service.

Step 2: Analyze the Contract: What's Off-Limits?

Confidentiality obligations can exist in multiple places in a document, so read through the language carefully!

A. Where to Find the Language

Scan your agreement for these clauses. They may create confidentiality obligations in specific ways:

- **Confidentiality:** Typically outlines the scope of your obligations based on the definition of "Confidential Information".
- **Payment & Pricing:** Might restrict you from sharing rates, royalties, or fee structures.
- **Term & Termination:** Often describes how long any confidentiality obligations will last. Look for "survival" language here, which can extend the confidentiality term beyond the end of the rest

of the contract.

- **Publicity / Marketing:** Might limit what you can say publicly about the relationship.
- **Grant of Rights:** Might restrict how you describe the licensed material, but might only restrict what you can use it for.
- **Deliverables / Work Product:** Some work product might be considered "confidential" until it's publicly released (like a newly-developed game), but some or all aspects of that confidentiality might expire upon release. For example, the existence of the work product would be publicly known, but the details of funding or development might still be confidential.

B. Keywords

If you don't see a "Confidentiality" header or language in the clauses above, Ctrl+F for:

- **Proprietary**
- **Trade Secret**
- **Restricted**
- **Shall not disclose**
- **Confidential**

C. The Analysis Checklist

Use this mental model to extract the rules from your document:

- **The Definition:** Confidentiality obligations only apply to information that everyone agrees is confidential. Is "Confidential Information" defined broadly ("this contract and its terms") or narrowly ("only items marked Confidential")?
- **The Exclusions:** Does it explicitly exclude information that is Public, Already Known, Independently Developed, or Required by Law to be shared?
- **The Duration:** Is the obligation fixed (e.g., "3 years from disclosure") or indefinite?

Step 3: Categorize Your Data: Use the Decision Framework

Follow this Framework and use these Decision Points to evaluate and categorize the information you have. You can also use the appended Decision Flowchart to help filter that information; the logic below mirrors the decision points in the graphic.

First Decision Point: Is the Information Publicly Known?

- **The Test:** Is the information already available through an authorized public channel (e.g., the vendor's website, official press releases, or government records)? ***NOTE: even information that is widely discussed in a community isn't necessarily "publicly known."***
- **Yes: STOP.** This is low risk. You are likely free to share.
- **No / Unsure:** Proceed to Decision Point 2.

Second Decision Point: Is the Information Considered "Confidential" Under Your Contract?

- **The Test:** Check your contract, Terms of Service, or End User License Agreement ("EULA") language.
    - Does the definition of "Confidential Information" include the category of information you want to share?
    - Does any other clause in your contract concern the type of information you want to share, and if so, does that clause limit sharing?
- **No:** (e.g., the language only limits sharing user metrics, and you want to discuss your payment terms). **STOP**. This is low risk, and you are likely free to share, but exercise professional courtesy before you do!
- **Yes:** Proceed to Decision Point 3.

Third Decision Point: Is There an Applicable Exception?

- **The Test:** Check the "Exclusions" or "Exceptions" clause.
    - Did you already know this information before entering into an agreement?
    - Did you develop this information independently (e.g., your own metrics)?

    - Are you required by law (FOIA/court order) to disclose it?
- **Yes: STOP.** Low risk. You may share, but check for notification requirements (e.g., "prompt notice" to the third party).
- **No: STOP.** *This is likely restricted information, so proceed to risk assessment.*

Step 4: Move to Next Steps

If you reach the end of the Framework and you are unsure about whether your information really is confidential, you have two paths:

Path A: Consult Legal Counsel

Use these specific questions to get direct, high-value answers:

- **Before Entering an Agreement:** "Is the definition of 'Confidential Information' too broad? It seems to cover our own data."
- **Existing Agreement:** "I want to share [X], which I think is public knowledge. Does this fall under a standard exception, or any exceptions in Clause [Y]?"
- **Known Risk:** "We received a FOIA request for this contract. The terms say that the entire agreement is 'Confidential.' What do we need to do?"

Path B: Risk Assessment (No Counsel Available)

If you do not have immediate access to legal counsel, refer to the Risk Assessment Guide to evaluate the potential consequences of sharing the information.

Conclusion

Confidentiality obligations might appear tricky and onerous, but you can navigate them by following the steps above and referencing the flowchart in the appendix. When in doubt, assess your (and your organization's) risk in sharing the information you want to share (or consult qualified counsel!) before you proceed to share.

Risk Assessment Guide

Risk Assessment Guide

> ***Disclaimer: This guide provides a framework for analysis and is not legal advice. For specific ambiguities or high-stakes situations not covered here, consult qualified legal counsel.***

Risk is an inherent part of any business, from signing a contract with a new startup partner, making investment decisions, speaking publicly as an organization, or sharing information that might be considered confidential.

As information professionals, we use risk assessment every day: Imagine you're a public library director coming in to work on a snowy day. Your maintenance personnel are already snowed in and won't make it to clear the walkways. You take stock of the amount of snow, salt for de-icing, who can help, and whether you can ask them. Using that information, you decide to remain closed: the risk of injury to non-maintenance staff was too high to merit opening on time.

That's risk assessment in action.

This guide is a practical, step by step set of steps you can take to evaluate your risk as you make decisions on behalf of your organization. In short, this guide will help you to know what to do when you don't know what to do, particularly in contractual settings.

Situational Awareness is Key

Assessing risk means understanding your organization's position relative to the risk. Consider:

Core reputational and political effects:

- **Mission Alignment**: How will your decision affect members of your organization personally and publicly? What is your organization's mission or purpose, and is it implicated in this decision?

- **Public Stance**: If the organization's purpose is implicated, does the organization want to make a political statement or take a public stance?

For example: if your library organization is offered funds from a person or group known to actively support legislative acts that would censor or cull your collections on the condition that the donor can "occasionally audit" materials, accepting funds is directly counter to the mission of the library. The risk is far too great even if that audit might never take place. This ticks both the "Mission Alignment" and "Public Stance" boxes, as accepting funds would be a public statement in itself.

Direct organizational effects:

- **Contractual terms**: Would your organization be violating terms of a contract, and if so, does the organization care about losing that partnership, losing a core service, or paying for breach?
- **Financial resilience**: Is your organization prepared to accept a financial consequence beyond paying a termination fee or fine? What about potential court costs?
- **Safety of staff and patrons**: Does your organization have enough resources to protect individual staff and patrons from the effect of this decision? How are you supporting your community in the face of potential attacks?

The position of any third party or counterparty:

- **Litigation risk**: Does the decision involve a third party that's known to be litigious (prone to sue other companies) or has a "bully" reputation on social media?
- **Defense strategy**: Is your organization prepared to address or ignore a social attack? To what degree? If you're considering making negative statements about a third party, is your organization prepared to defend those statements?

Placing relative value on each answer will help you determine how to move forward. The Risk Exposure Scorecard below can be of use in that determination.

Risk Exposure Scorecard

Use this scorecard for any action you're considering where you aren't sure of the risk. This scorecard is meant to be copied and reused for each decision.

To use the scorecard, rate the **Risk Factor** in the first column based on how strongly you agree with its related **Statement** in the second column. Write your **Score** in the third column and add any **Notes** in the fourth column. Then **Total** your score in the last row.

Scoring Rubric:

1 – Strongly Disagree/non-issue

2 – Disagree or minor issue that can be managed

3 – Neutral, unsure or unpredictable

4 – Agree, likelihood that harm will result

5 – Strongly Agree, harm is certain and would be highly damaging

As you're scoring, you may be tempted to enter a lot of "3" scores. That's okay, but consider that if you're consistently neutral on the risk around a particular decision it might be worth getting a second or third opinion from a trusted colleague who's familiar with your organization's mission and policies.

A score of "2" indicates that you see reasonable, practical steps that your organization can take to manage the risk, while a score of "4" means that while you might see possible steps you can take, those steps will be burdensome and you'll need organizational signoff before acting.

Risk Factor	Statement	Score (1-5)	Notes
Mission Alignment	This action directly conflicts with our public mission or core values.		
Operational Dependency	Another party provides a service or level of support that we cannot easily replace if they terminate the relationship.		
Third Party Reputation	Another party has a known history of taking people to court or using "bully" tactics on social media.		
Financial Exposure	A legal battle or high fine could result from this action, and our organization may not be/is not prepared for either circumstance.		
Defensibility	Our organizational leadership or guidance does not give us a clear professional, ethical, or legal reason to justify this action.		
TOTAL SCORE			

Interpreting the Score:

Warning: An individual score of **4** or **5** for any Risk Factor is a red flag. *Share your results with and obtain informed consent from organizational leadership before proceeding.*

If you don't have any 4 or 5 scores, use the Total Score analysis below:

Total Score 5–10 (low risk): Your organization is likely protected by its policy or standard practices. The risk is low – but be sure to document your reasoning.

Total Score 11–14 (mitigation needed): Consider how to mitigate before proceeding: can you anonymize relevant data, delay timing, narrow the scope of who sees information, or pursue alternative actions like private discussions instead of public statements?

Total Score above 15 (high risk): As any score above 15 means you'll have entered a 4 or 5 for at least one Risk Factor, review your results with organizational leadership and obtain consent before proceeding. Ask:

- If you have one "4" in a sea of 1 or 2 scores, can you work to mitigate the "4"?
- If you entered a "5" anywhere, how certain are you of the resulting harm?

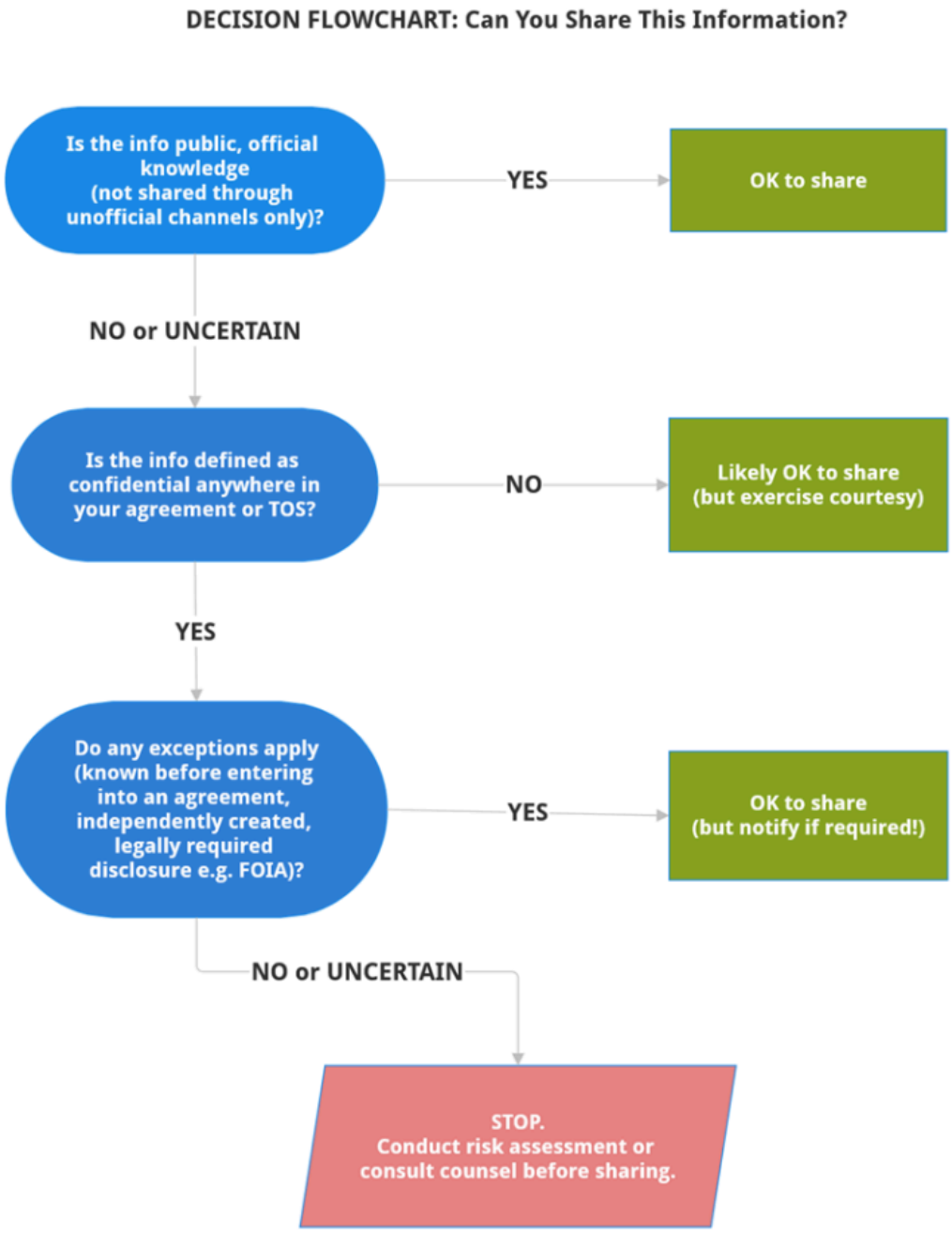
Regardless of your organization's decision, always document the review and decision-making process so that you can reference it later when necessary.

Some organizations might choose to proceed even knowing the risk is high out of principle or value alignment; others might choose to abstain even knowing the risk is low because they're not able to bear even a slight financial burden. What's most important is to make informed decisions about risk and provide reasoning behind your decisions.

As always, if you or your organization are stuck on a decision, consult qualified counsel.

Appendix 1: Decision Flowchart

See [Step 3: Categorize Your Data: Use the Decision Framework] for a text-based version of this flowchart.



Appendix 2: Sample Services Agreement

This is an example of a contract that a technology provider might offer you. You'll find important language affecting your ability to share information relating to this relationship in a few different locations throughout the contract, all of which can inform your risk analysis. If you're in the negotiation stage, knowing how to identify this language can also inform your negotiations.

Annotations, including explanatory notes and Q&A, appear in italics throughout the document.

SERVICES AGREEMENT

This Services Agreement (**"Agreement"**) by and between Super Software Co. (**"SSC"**) and the subscriber named in Section 1 (**"Subscriber"**) (together the **"parties"**), effective as of the date of the last signature below (**"Effective Date"**), outlines the terms and conditions under which SSC will provide services to Subscriber. For good and valuable consideration the sufficiency of which is acknowledged, the parties agree as follows.

SECTION 1. DEFINITIONS

1.1 "Confidential Information" means all non-public information disclosed by SSC to Subscriber, whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Confidential Information includes, without limitation, software code, dashboard designs, business roadmaps, and the methodology of the SSC "BestRank" ranking algorithm.

Q: Is "Confidential Information" an exhaustive list?

A: Not necessarily! Be on the lookout for other expectations around confidentiality.

1.2 "Subscriber" means [the subscriber's name and contact information].

1.3 "Subscriber Data" means any data owned by Subscriber at the time the parties enter into this Agreement or that comes into being during the Term of the Agreement and is not a product of Subscriber's use of SSC services.

Q: Does "Subscriber Data" qualify as "Confidential Information"?

A: No, even if the Subscriber would consider that data to be protectable. It probably is, but it's not covered by the above definition, so SSC doesn't have any expectations around it for the purposes of this contract.

SECTION 3. FEES AND PAYMENT

3.1 Fees. SSC shall calculate fees at the rate indicated on the related invoice. All invoices and Fee information are considered "Confidential Information" under this Agreement.

Note: The "Fees" clause expands "Confidential Information" in this contract, so any terms that apply to "Confidential Information" also apply to invoices and Fee information.

3.2 Payment Terms. Subscriber shall pay the Fees indicated on the related invoice net thirty (30) days of receipt of that invoice.

SECTION 4. NON-DISCLOSURE

4.1 Duty of Confidentiality. Subscriber shall use the same degree of care to protect Confidential Information as it uses for its own similar information. Subscriber shall not disclose or use any Confidential Information of SSC for any purpose outside the scope of this Agreement.

Q: What is Subscriber prevented from doing with Confidential Information?

A: Per these terms, Subscriber would need to protect Confidential Information (as defined above, plus the Fee addition in Section 3.1) in the same way it would protect its own information, and must not disclose that information for any reason – so this is a very restrictive duty.

4.2 Exceptions. The obligations in Section 4.1 do not apply to information that:

(a) is or becomes generally available to the public through no fault of the Subscriber;

(b) was already in the Subscriber's possession without an obligation of secrecy;

(c) is independently developed by the Subscriber; or

(d) is "Subscriber Data" as defined in this Agreement.

Q: How do these Exceptions change the duty above?

A: This clause carves out the types of exceptions that usually apply to confidentiality restrictions: it doesn't give Subscriber a lot of leeway in terms of sharing SSC's information.

SECTION 7. INDEMNIFICATION

7.1 Subscriber Indemnity. Subscriber shall indemnify, defend, and hold harmless SSC from and against any and all claims, damages, or losses arising out of Subscriber's unauthorized use of the SSC services or any breach of this Agreement.

Note: Indemnification, or indemnity, clauses are usually "standard" terms in a template. It basically means you're not going to sue the company if something goes wrong. They're not a big part of a confidentiality assessment, but they're worth reviewing and pushing back on because they tend to be one-sided by default.

Pro Tip: Ask the other party to make indemnification mutual. If they refuse, that's a good indicator that the terms aren't well written. You can negotiate by suggesting edits that make sense for your situation.

SECTION 9. TERM AND TERMINATION

9.1 Term. ...

9.2 Termination for Cause. Either party may immediately terminate this Agreement if the other party materially breaches any term. For clarity, Subscriber's failure to protect Confidential Information is considered a material breach and grounds for termination by SSC.

9.3 Termination for Convenience. SSC may terminate this Agreement at any time, for any reason or no reason, upon sixty (60) days' prior written notice...

9.4 Effect of Termination. Upon termination or expiration of this Agreement, Subscriber's access to the SSC Dashboard and all SSC services immediately ceases and Subscriber shall return all materials, including but not limited to any Confidential Information, received from SSC which are not demonstrably required for Subscriber's ongoing business purposes following termination. In the event that SSC terminates this Agreement under Section 9.2, SSC may in its sole discretion seek monetary damages not to exceed the total value of this Agreement.

SECTION 10. GENERAL PROVISIONS

10.1 Survival. Sections 1 , 3.1, 4, 7, 9.4, 10, and any provisions that by their nature survive, survive expiration or termination of this Agreement. The obligations in Section 4 remain in effect for a period of three (3) years following termination.