DIATYPOSIS

The Digital Integrity & Safety Audit

A self-assessment for mission-driven organizations to ensure their technology protects their community.

Table of Contents

Ethical, inclusive design for organizations built around people.

I'm Kristi-Lynn, the founder of Diatyposis, a digital design studio focused on privacy, accessibility, and ethical design. I bring two decades of senior UX and digital product experience to human rights and community organizations that need it most—helping them build digital spaces that are inclusive, secure, and as thoughtful as the work they do.

My work is guided by DIATYPOSIS—a rhetorical principle of offering clear, structured guidance so people can make informed choices. In practice, that means designing tools that are transparent, private, and easy to understand. Whether you're providing reproductive healthcare, LGBTQ+ support, or community resources, your digital presence becomes a safe, reliable bridge to the people who need you most.

This guide is designed to help you understand and assess how well your website is performing for accessibility, safety, and privacy. I hope this guide gives you some clarity about what your organization is doing well and where your organization may be able to improve.

Take your time with this process. It can take years to get it all right, but it's worth the effort to ensure your website is aligned with your mission!

Kristi-Lynn

Phase 1: Data Collection & Minimization

THE “WHY” TEST

We want to collect (and store) as little information as possible from our users. When asking for personal information, it’s important to ask ourselves: “Why are we collecting this?” and “If this were to be leaked or stolen, what harm could come to the people we serve?”

Look at your most used contact, intake, and/or donation form. Do you collect any data point (Phone, Address, Last Name) that is not strictly necessary to provide the immediate service?

- [ ] We only collect data points (Phone, Address, Last Name) that are essential to the immediate service being provided.

NOTES

THE EXPIRY POLICY

How long does your organization hold on to user data? Ideally, all records should expire at some point—it’s up to your organization to decide when. This should be detailed in your privacy policy (e.g., "All intake records are purged 30 days after the case is closed.")

- [ ] We have an established schedule to delete sensitive intake records once they are no longer legally or operationally required.

NOTES

THIRD-PARTY LEAKAGE

Websites rarely run without any third-party involvement. These third parties could include analytics services, form collection, fundraising platforms, CRMs, and even the service that hosts your website. Are you using "free" tools like Google Forms or Typeform for sensitive data? (These often track user metadata even if you don't.)

- [ ] Our intake forms and data collection tools are hosted by privacy-first providers that do not track or sell our users' metadata.

NOTES

COOKIE CONSENT

Cookies are small bits of data that are stored on a users' computer that can save information about what pages they visit, what actions they take, and what settings they prefer. It would be more accurate to call them 'trackers' than 'cookies,' but one way to think about them is more like a Hansel-and-Gretel-style trail of cookie crumbs you leave around the internet.

Cookies should not be set unless a user actively accepts them, and cookieless analytics providers like Fathom or Plausible limit the amount of data collected about your users.

- [ ] Our website does not track cookies before a user consents.
- [ ] Our website uses cookieless analytics.

NOTES

Phase 2: User Safety & Trauma-Informed UX

THE “QUICK EXIT”

We want to protect users who may be browsing your website in a high-stakes or monitored environment. If your organization handles sensitive topics (domestic violence, reproductive health, LGBTQ+ support), a persistent "Exit Site" button that immediately redirects to a neutral page like Google or Weather.com can save lives.

- [ ] Our site features a visible "Quick Exit" button for users who may be in a monitored or unsafe physical environment.

NOTES

BROWSER HISTORY GUIDANCE

Helping your users understand how to clear their history or use a private browser window is a great way to ensure their privacy can be maintained wherever they are. Do you provide a clear, easy-to-find link explaining how to browse in "Incognito/Private" mode or how to clear history?

- [ ] We provide a clear, jargon-free guide on our site explaining how users can browse privately and clear their history.

NOTES

INCLUSIVE ACCESSIBILITY

Websites should be accessible by everyone visiting them. Visitors with vision disabilities may access your site using a screen reader, visitors with mobility disabilities may need keyboard controls to navigate easily, deaf or hard-of-hearing visitors may need captions on video content, and visitors with hidden disabilities like autism or ADHD may prefer limited animations. Some users may be using older devices with more limited capabilities.

The Web Content Accessibility Guidelines are a great tool to assess the accessibility of your website including visual contrast and usability.

- [ ] Our site meets WCAG 2.2 standards, ensuring it is usable by everyone, regardless of ability or device age.

NOTES

PRIVACY-FIRST SHARING

Social media share buttons and embeds include what are called ‘tracking pixels.’ These tracking pixels ping the source website (e.g. Facebook) whenever that page or item is loaded on your website. This is another form of third-party tracking, and your website may be sending information about your visitors’ location, device type, and activity on your website back to the social media company. These should be removed whenever possible.

- [ ] Our website does not use social media tracking pixels or "share" buttons that monitor users without their consent.

NOTES

Phase 3: Internal Infrastructure

ADMIN HYGIENE

It’s essential to know who has access to user data and remove that access as soon as possible when it’s no longer needed. When was the last time you audited your website or database logins? Are there former employees or volunteers who still have "Owner" access?

- [ ] We perform quarterly audits of our admin accounts and have revoked access for all former staff and volunteers.

NOTES

ENCRYPTED COMMUNICATIONS & SILOING

It’s important to use communication services that are encrypted whenever possible, and only include staff in conversations that are immediately relevant to them.

End-to-end encryption ensures that communications can only be read by the person sending them and the person receiving them. Services like Signal can replace text messages for encrypted conversations, and email services like ProtonMail provide end-to-end encryption between ProtonMail accounts.

- [ ] All sensitive client and internal discussions happen over end-to-end encrypted channels (e.g. Signal or ProtonMail).

NOTES

DIGITAL FINGERPRINTS & METADATA SCRUBBING

Every digital file—whether it’s a photo, a PDF, or an email—contains “metadata” that acts as a digital fingerprint. This can include the GPS coordinates of where a photo was taken, the name of the person who created a document, or even the internal file paths on a staff member’s computer.

Scrubbing this data ensures that you aren't accidentally leaking sensitive information to the public or to “Big Tech” trackers. For mission-driven organizations, this also means self-hosting website assets like fonts and scripts, so that a user’s visit to your site isn’t “pinged” back to third-party servers like Google or Adobe.

- [ ] All public-facing PDFs and documents are scrubbed of author names, local file paths, and revision histories.
- [ ] We self-host all fonts and scripts to prevent “pinging” third-party servers (like Google or Adobe) when a user visits our site.
- [ ] We strip metadata (GPS and timestamps) from all photos before they are uploaded to the web or social media.

NOTES

Does your digital presence match your mission?

If this audit revealed gaps between your values and your technology, you don't have to navigate the fix alone. I help mission-driven organizations build digital spaces that are secure, inclusive, and built to last.

Every organization has different constraints and goals. If you're looking for a partner to help navigate these privacy and access challenges, please get in touch so we can discuss a path that works for your unique situation.

START A CONVERSATION