How to Secure Private and Confidential Data

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Your nonprofit works hard to build trust with the people and communities you serve. To maintain that trust, you must safeguard the data that clients, constituents, partners, website users, and others share with you. Many nonprofits don't have an on-site cybersecurity expert, but creating and applying some simple data security principles can make a big difference. With that foundation, your nonprofit can continue to improve its data security as best practices change. Here's how to get started.

Take inventory. What personal or confidential data does your nonprofit currently have? Whether it's Personally Identifiable Information (PII), Protected Health Information (PHI), or confidential information, where and how do you store it? What user data does your organization possess that it needs to keep private? Who do you need to protect that data from? What are the consequences if you fail? What safeguards do you have in place, and are they sufficient? The Electronic Frontier Foundation has a guide that can help your nonprofit explore these questions in detail.

Limit data collection. Don't collect data your organization doesn't need or use. Hackers can't steal data your organization doesn't possess.

Nail the basics. Require strong passwords for internal and external system and site users. Set up multi-factor authentication, which requires additional information beyond a login and password (like a code sent to your cell phone) to access systems. Require your nonprofit's vendors to take steps to protect data.

Get encryption. Make sure your office's network is encrypted and secure. Never use public networks to access your nonprofit's data. Store any financial information or other sensitive data, including donor and client names, in an encrypted database. Never store data like financial details or passwords in plain text.

Limit internal access to sensitive data. Give employees access only to the data they need to perform their jobs, and make sure only authorized users can access sensitive data. Limiting access allows you to spot any unusual activity more easily.

Don't snooze software updates. Updates often contain critical patches for security issues. Regular updates are especially important if your organization's website is built on WordPress, as many nonprofit sites are. WordPress's popularity makes it a frequent hacker target.

Be transparent. Clearly and prominently describe what data your nonprofit stores and what you do with it. Create privacy policies covering all your services that show what donor, participant or site visitor information you record and why. Allow website users to opt in to data collection, rather than requiring them to opt out. Give them the opportunity to request a copy of their data. If your nonprofit uses algorithms to make decisions, explain how and when you do so.

Consider limiting or turning off user tracking on your website. If you don't know what tracking your site uses, the Electronic Frontier Foundation's Privacy Badger browser extension can show you.

Avoid data sharing whenever you can, and limit it in all cases. Before your organization shares data with anyone, set guidelines on how the data can be handled. Create a policy on what kinds of data you will share and

with whom.

Think about data retention. Your organization may want to automatically delete data as often as it is reasonable.

Resources

- Online Privacy for Nonprofits – Electronic Frontier Foundation
- How to Keep Your Donor Data Safe – Nonprofit Hub
- Data Policies Your Nonprofit Needs – NTEN
- Data Protection: 7 Proactive Ways to Protect Your Organization – North Carolina Nonprofits