Nonprofit Risk Management Center

VOL. 35 • NO. 2 • SUMMER 2026

Risk Management ESSENTIALS

Tips, Knowledge and Tools for Nonprofit Organizations

2026 Risk Summit: Ready, Resilient, Risk-Aware

The 2026 Risk Summit at the Hyatt Regency Reston November 5 and 6 is an in-person gathering showcasing innovation in nonprofit risk management. This premier educational event will bring together nonprofit leaders and professionals to explore emerging risks, practical solutions, and forward-thinking strategies.

Attendees will participate in timely educational sessions, meaningful peer-to-peer learning, and ample opportunities for in-person networking. Don't miss the conference reception on the evening of November 5th for more connection, collaboration, and relationship-building with like-minded sector professionals.

Visit 2026risksummit.org to learn more about the summit and register.

Call 703.777.3504 or email info@nonprofitrisk.org for more information.

Smart Cybersecurity Measures Any Nonprofit Can Take

By Rachel Sams

The email came from someone I knew. It linked to a document I was expecting to receive. But the link looked bland and generic—the way examples of phishing scams look.

I was tired. I wanted to click, get the document and get on with my day.

I thought about the Take 9 campaign from Craig Newmark Philanthropies ("Take a 9-second pause and think before you click, download, share.") OK, I thought, I can take 9 seconds.

When those 9 seconds were up, I knew I should dial the phone, just to check. So I did. I left my contact a voicemail. They responded right away, sounding surprised to hear from me but glad to confirm they sent the document.

Double-checking where that link came from cost my nonprofit zero money and very little time.

I might click a malicious link or attachment someday. Anyone might. But plenty of free or low-cost steps like the one above can help your team strengthen its

CONTINUED ON PAGE 2

A PUBLICATION OF THE NONPROFIT RISK MANAGEMENT CENTER
204 South King Street, Leesburg, VA 20175 | 703.777.3504 | www.nonprofitrisk.org
©2026 Nonprofit Risk Management Center

Risk Management
ESSENTIALS

VOL. 35 • NO. 2 • SUMMER 2026

Published periodically by the
Nonprofit Risk Management Center
204 South King Street, Leesburg, VA 20175
Phone: 703.777.3504
www.nonprofitrisk.org

Staff Directory
(All staff can be reached at 703.777.3504)

MELANIE LOCKWOOD HERMAN
Executive Director
Melanie@nonprofitrisk.org

ELYZABETH JOY HOLFORD
Assistant Executive Director
elyzabeth@nonprofitrisk.org

RACHEL SAMS
Lead Consultant and Editor
Rachel@nonprofitrisk.org

WHITNEY CLAIRE THOMEY
Lead Consultant
Whitney@nonprofitrisk.org

2026 Board of Directors

President
Joseph A. Budzynski
Volunteers of America

Treasurer
Kemba Esmond
NeighborWorks America

Secretary
Dr. Jermaine L. Hunter
Melwood

Paul Doman

David S. Kyllo
Kyllo Consulting

Lisa Prinz

Julie Reyburn
Episcopal Relief & Development

Michael A. Schraer
Chubb

Patricia Vaughan
Population Council

Smart Cybersecurity Measures Any Nonprofit Can Take

CONTINUED FROM PAGE 1

cyberdefenses and make it more likely that you can consistently keep your nonprofit's data safe.

Why Cybersecurity Matters

If you think your nonprofit doesn't have any data cybercriminals would want, think again.

All nonprofits collect personally identifiable information. Your digital and paper files are likely full of phone numbers, email addresses, and physical addresses of clients, team members, volunteers, and more. Somewhere in your systems, you likely store even more sensitive information, like credit card numbers and bank account data. You may have demographic information about the ethnicity or gender of participants, volunteers, and staff.

> "If you think your nonprofit doesn't have any data cybercriminals would want, think again."

Every piece of that information belongs to a person: a valued team member or client. That means your mission includes protecting those people's data from misuse.

Common examples of cybersecurity breaches nonprofits experience include:

- Social engineering "phishing" scams like the one I suspected in the example above. If you've ever received an email that appeared to come from your CEO, pleading with you to issue gift cards to someone immediately, you've experienced a phishing attempt. Social engineering uses emails, texts or social media messages to prompt users to reveal sensitive information or access a malicious link or attachment. In "spear phishing," attackers tailor these attempts to a person based on information from their public social media or publicly available profiles.
- Malware, or software that can disable computer systems, destroy or steal data, and more. This category includes ransomware, in which the attacker demands a ransom to get data back or systems operating again.
- Denial-of-service (DOS, or DDOS for larger-scale distributed-denial-of-service) attacks flood an organization with electronic traffic until its systems can't respond to routine requests.

Start with Humans

How do you address the risks of those types of cyberattacks?

The human beings in your organization are its strongest and weakest link when it comes to cybersecurity. Your team members' quick thinking could thwart an attack, while one seemingly small mistake could compromise your entire network and cost you millions of dollars. To fortify your cyberdefenses, it makes sense to start with your people.

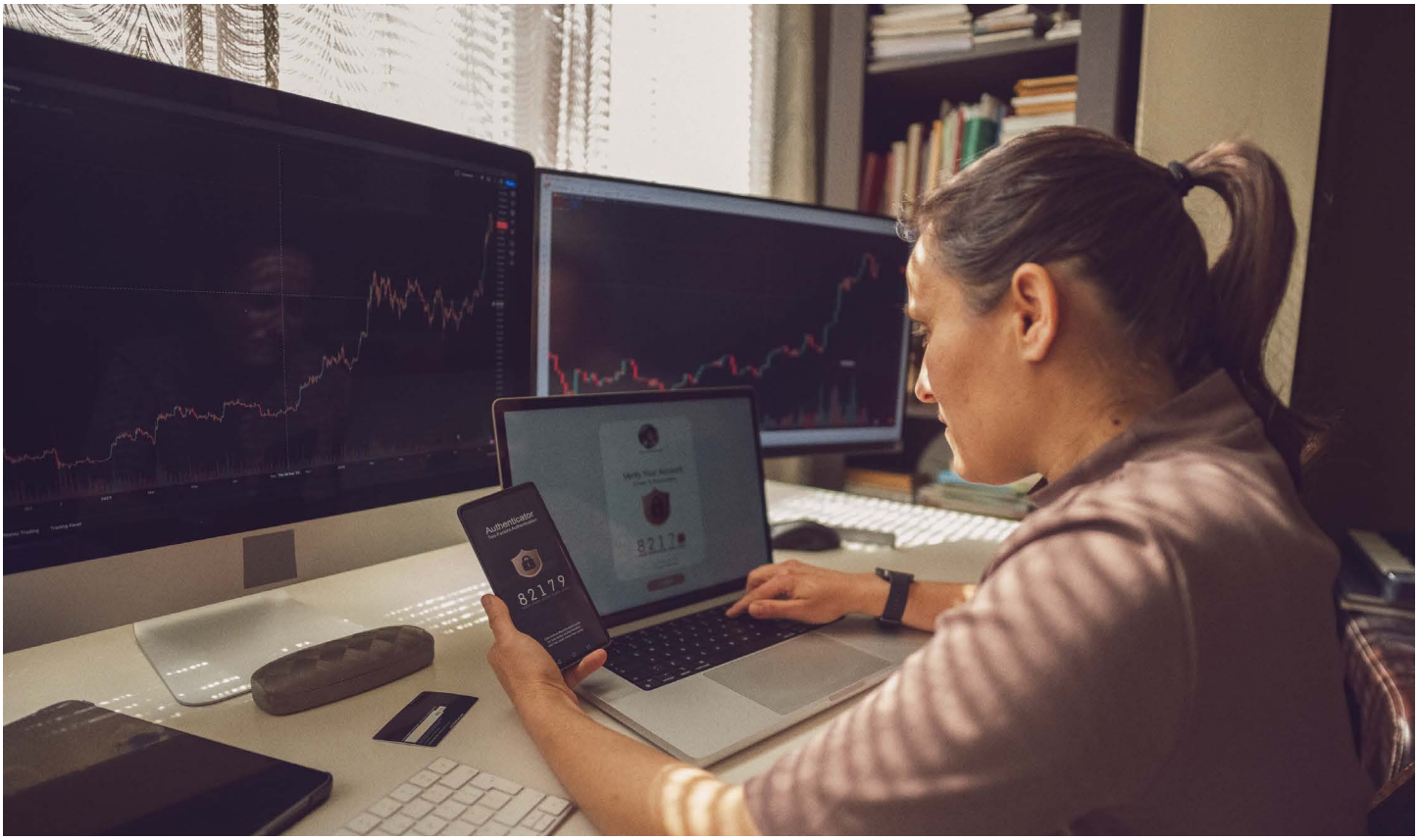
If you don't already send your team members phishing simulations, where a third party tests them on how they would respond to common social engineering scenarios, that's a great place to start. Your IT provider may be able to provide these as part of your existing relationship, or you may be able to take advantage of these features in software like Microsoft Defender. You can

> "The human beings in your organization are its strongest and weakest link when it comes to cybersecurity."

CONTINUED ON NEXT PAGE

Smart Cybersecurity Measures Any Nonprofit Can Take

CONTINUED FROM PAGE 2



also access free resources like KnowBe4's option to send free phishing simulations to up to 100 users.

Some great cybersecurity practices to instill in your team:

- Hover over links and check sender addresses before responding to an email, clicking a link or downloading an attachment.
- Verify requests like wire transfers, gift cards or password resets through another channel. If the request came by email, reach out to the purported sender by phone or another means to confirm they sent the message.
- Create and share a clear process for how employees who suspect they've been phished or your systems have been compromised can report their concerns.
- Use free videos from your Internet provider or other credible sources to reinforce what your team is learning about cybersecurity.

Build on the Basics

Make sure your nonprofit has the basics in place on passwords and multifactor authentication to reinforce system security, too.

- Require long, complex passphrases.
- Don't allow password reuse across systems, and don't let employees share passwords with other users.
- Use a password manager like LastPass, 1Password or Dashlane to help team members create strong passwords and securely store them.

Multifactor authentication provides an extra layer of security for your organization's accounts. At its simplest, multifactor authentication requires additional information beyond a login and password to access organizational systems—for example, a number entered

CONTINUED ON PAGE 4

Smart Cybersecurity Measures Any Nonprofit Can Take

CONTINUED FROM PAGE 3

> "Store documents in approved cloud software with access controls rather than local copies on personal devices."

from an authentication app. Multifactor authentication creates additional hurdles for outside actors to break into a system; they'd need not only your login and password, but also the authentication code.

Organizations should consider and address the potential for bias in multifactor authentication. Concerns about that have led some nonprofits to avoid authentication options that involve facial recognition. Of the major biometric authentication methods in use, facial recognition is the least accurate, raises extensive privacy concerns, and current implementation of the technology "involves significant racial bias, particularly against Black Americans," according to Harvard.

Here are some additional steps to strengthen your cyberdefenses.

Update software, firewalls, and email filters regularly. I know—it seems like those update messages pop up every day. But taking a few minutes for updates can save hours, days, or weeks of headaches down the road. Software updates can patch vulnerabilities hackers could use to get into a product. They also help protect the personal information on your devices. Encourage your team members to set reminders to download updates when they step away from their computer for lunch or a break.

Remove old user accounts when staff or volunteers leave your organization. Make sure you revoke all their accesses to your systems, from email to shared drives. Create a standardized process for this, so team members aren't scrambling every time someone leaves.

Standardize where you store files in your organization. Store documents in approved cloud software with access controls rather than local copies on personal devices.

Create tiered data access. Make sure that only employees who need to access

CONTINUED ON NEXT PAGE

Smart Cybersecurity Measures Any Nonprofit Can Take
CONTINUED FROM PAGE 4

specific data, especially sensitive data, have the ability to do so.

Restrict who can install software on organizational devices. Check that your process is simple and seamless. Don't incentivize the action you're trying to avoid: staff downloading software on their organization-issued laptops because it 'takes too long' to get help from the colleague assigned to help.

Set security standards and protocols for employees who access your organization's computer system from home or on the road. Make these standards and protocols simple, jargon-free and easy to access.

Collect only the data you really need. Stop collecting data you can't or won't use! And follow a practical schedule and protocol for data deletion. If your organization doesn't collect it, hackers can't steal it (at least not from you!)

Cyberbreaches: Get Ready to Be Ready

The bad news: Your nonprofit could take all the above steps and still experience a data breach. Cybercriminals are persistent, and they constantly evolve their tactics, including using artificial intelligence to help infiltrate systems.

The good news: If you've taken the above steps, you're likely to incur less damage in a breach. And if you take a little time now to prepare for what you would do in the event of a breach, that stressful time will be less painful. Here are some steps to help.

Identify now who your team will call if a cybersecurity breach occurs. Cyber insurance providers often have "breach coaches" who can lead an insurance response for nonprofits. Put your legal counsel on the list of people to call, along with any cybersecurity law or forensic experts your counsel recommends. Your list might also include your information technology and security vendors, operations, human resources, communications, and management.

Identify which systems and data are mission critical. What systems would render your organization inoperable if you didn't have access to them? Make sure you have backups in place on those systems. This may happen automatically through your software programs. Double-check whether it does, and if not, make the necessary backup provisions.

Craft a contingency plan. What work could you do if your organization's major digital systems were unavailable? Who would lead your response to a cyberbreach, and who is that person's backup?

Keep Learning, Keep Preparing

If you've read this far, you know cybersecurity isn't one and done. Like so many things in our nonprofit organizations, improving our cybersecurity is a journey. If you put some basic safeguards in place, create a plan to keep learning, and share and discuss what you learn, you'll be well on your way to improved cyberhygiene.

Rachel Sams is Lead Consultant and Editor at the Nonprofit Risk Management Center. She is a firm believer in the power of the firewall update on a lunch break. Reach her with thoughts and questions about this article at rachel@nonprofitrisk.org or (505) 456-4045.

"Cybercriminals are persistent, and they constantly evolve their tactics, including using artificial intelligence to help infiltrate systems."

The PHLY *Difference*

Our specialty is that non-profit educational space. PHLY makes us better at it."

Philadelphia Insurance Companies provides specialized, innovative protection to educational institutions in the non-profit and human services space. Coverages include private, academic, religious, vocational and charter schools. PHLY offers separate limits for General Liability, Educators Professional and Cyber Liability, Abuse & Molestation. Learn more. Experience the PHLY difference.

PHILADELPHIA INSURANCE COMPANIES

A Member of the Tokio Marine Group

Call 800.873.4552
Visit PHLY.com

Michael R. Jakob
Principal
Carriage Trade
Insurance Agency, Inc.

AM Best A++ Rating | Ward's Top 50 2001-2025 | 96.7% Claims Satisfaction | 120+ Niche Industries

Philadelphia Insurance Companies is the marketing name for the property and casualty insurance operations of Philadelphia Consolidated Holding Corp., a member of Tokio Marine Group. All admitted coverages are written by Philadelphia Indemnity Insurance Company. Coverages are subject to actual policy language.

Forbes 2026 AMERICA'S BEST MIDSIZE EMPLOYERS

How to Create a Nonprofit AI Policy

By Rachel Sams

Do thoughts like these pop into your mind as you sit in traffic or scroll social media?

I wonder what my colleagues are doing with AI.

Are they doing things our nonprofit might not approve of?

Not even on purpose, just because...what the heck WOULD our nonprofit approve of doing with AI? Nobody's ever told us.

If these thoughts sound familiar, your nonprofit might need an AI policy.

Artificial intelligence—a broad term for technology that allows computers and machines to respond to input similarly to how humans do—is shaking up workplaces around the country, including nonprofits. The Chronicle of Philanthropy Technology Leadership Survey recently found that 46% of nonprofits are using AI and 77% expect to use it in the next three to five years.

But recent surveys estimate the percentage of nonprofits that have an AI policy at 10 to 15 percent. Luckily, that's a gap you can fill.

An AI policy can give your organization a foundation for how to use this technology in ways that support your mission and values, and avoid uses that would conflict with your mission. In this article, we'll explore how an AI policy can benefit your organization, how to create one, and what to include.

Startling Truths About Workplace AI Worries and Wants

Your employees—the very people who probably complain about some of the policies you already have, and may not always comply with them—might *want* an AI policy.

The nonprofit employees we talk to have concerns about AI, from its environmental impact to its potential for harm in society to whether it will take their jobs. Some nonprofit employees also worry that their organizations aren't using AI *enough*, and will fall behind on their ability to innovate and serve clients. And we've heard from employees at all points on that continuum who just want to know what their boss expects of them on AI and how they can and can't use it.

> "Artificial intelligence is shaking up workplaces around the country, including nonprofits."

An AI policy can help team members understand why you're spending time on this; know the limits of how they can use the technology; and navigate challenging

CONTINUED ON PAGE 8

How to Create a Nonprofit AI Policy
CONTINUED FROM PAGE 7

> "An AI policy helps your team understand the rules of the road and operate within them."

questions that arise. And nonprofits need that foundation sooner than later.

A recent survey by the firm Resume Now across all workplaces, not just nonprofits, found that nearly 60% of workers admitted to using AI in ways that might not meet company policy.

On the other hand, a study by generative AI platform Writer found that a third of respondents were refusing to adopt their company's AI tools. Many of those people indicated they didn't believe the technology was useful.

An AI policy helps your team understand the rules of the road and operate within them. It helps your organization think through what uses of AI would align with your values and which ones you absolutely want to avoid.

So what the heck do you put in your policy?

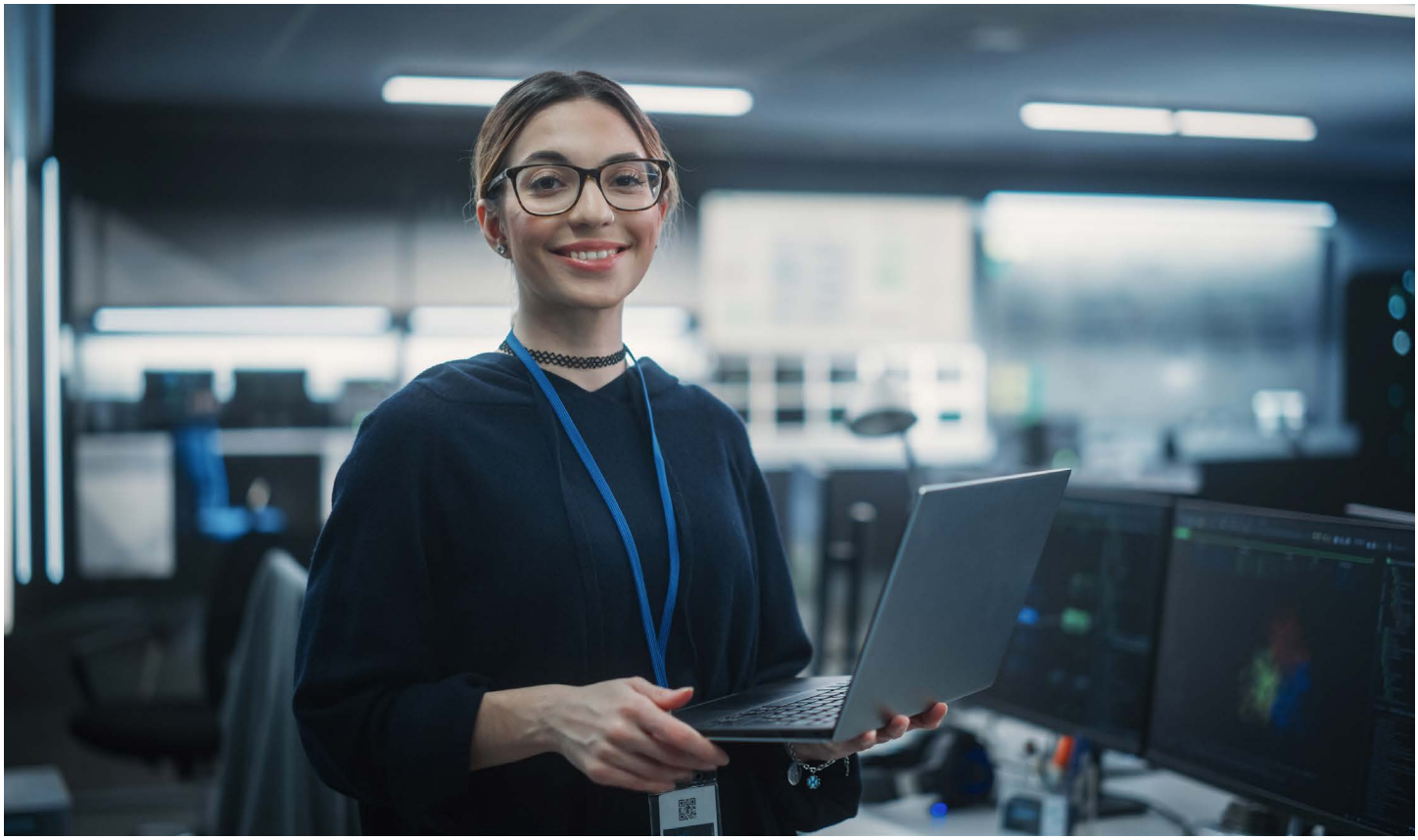
First, Know Your Purpose

Sometimes nonprofit leaders NRMC works with send us their AI policies for feedback. I see lots of things teams are doing well and plenty of areas to keep improving their policies. There is one area I find myself redlining in almost every single AI policy we receive.

That section is the *purpose*. The purpose section of most draft policies we review says something like, "We've created this policy because AI has a boatload of risks." That's fair, accurate, and important. Your policy should include a discussion of AI's concerning risks. What I don't typically see in draft policies is a positive statement of what organizations hope to do by bringing AI into their work. What good work do you hope to do with AI that you couldn't do without it?

Without some positive element in your statement of purpose, you'll have a hard time getting employees to even read your

CONTINUED ON NEXT PAGE



policy, let alone comply with it and spend time on training to get up to speed on AI.

Here are a few examples of policy language we've helped nonprofits craft to convey the positive things they hope to do with AI.

- Some of our team members have expressed a desire to use these technologies in ways they believe will help our organization innovate and improve.
- AI technologies hold the potential to automate some of our team's repetitive and time-consuming tasks and give us more time to do what we do best: serve children and families.
- We seek to use AI in ways that support our work, benefit our team and constituents, and protect employees, clients, and community members we work with from harm.

Beyond Purpose: Get Into the Details

Purpose is just one area you'll want to consider including in your AI policy. There *are* a boatload of risks that come with using AI, and your team needs guidance to navigate them. Other areas to consider including in your policy:

What kinds of AI use are encouraged, and within what parameters. What AI uses fit with your nonprofit's mission and values?

What kinds of AI use are prohibited. What behaviors and uses will your nonprofit not allow under any circumstances?

How your organization will train, equip and educate team members to use AI. How will you work with your team to find out what skills they want to develop and help them do that within your budget?

How you will preserve the security and privacy of data in your AI use. What practices will you use to safeguard sensitive data?

What security requirements will you have for AI services, vendors and products?

What will you do if data is breached?

When and how will you use informed consent?

How can constituents opt out of their data being used with AI?

When and how you will disclose your nonprofit's use of AI to internal and external audiences. How will you document and communicate your use of AI?

What measures you will take to ensure accuracy and mitigate or avoid bias in your use of AI.

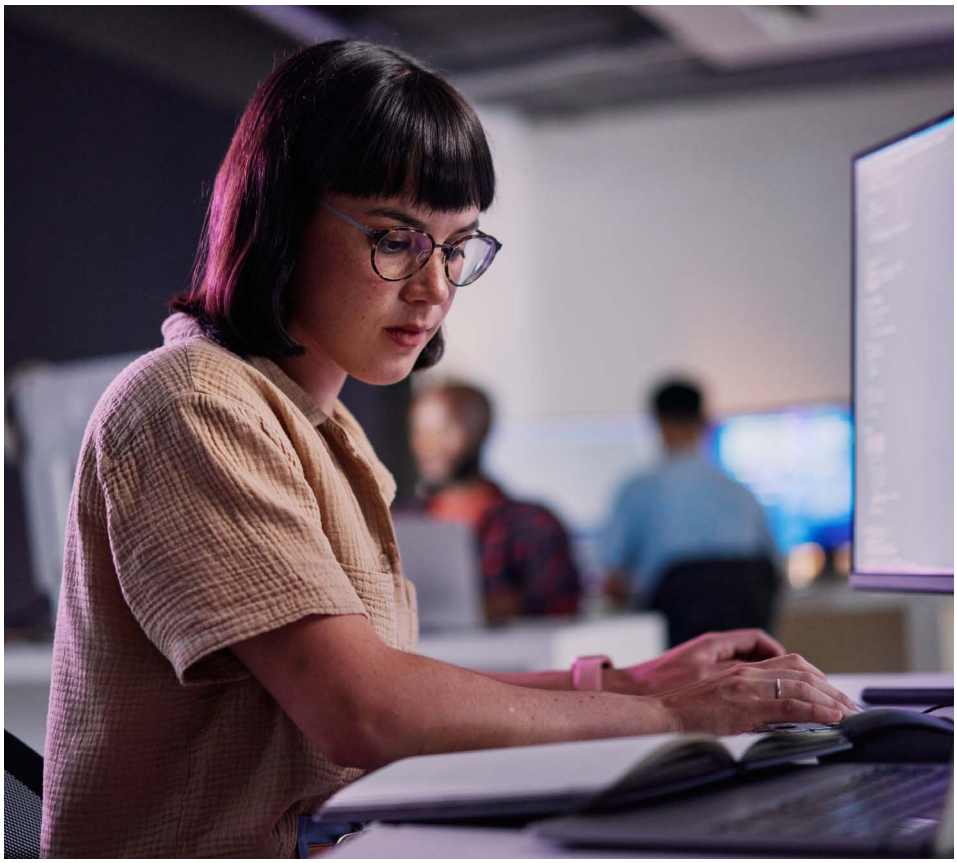
How will you educate your team about potential AI biases and check for them?

How will you ensure that a diverse group of constituents reviews all AI-generated work?

What will you do if bias is found in AI-generated work, before or after the fact?

CONTINUED ON PAGE 10

How to Create a Nonprofit AI Policy
CONTINUED FROM PAGE 9



> "How do team members feel about AI use? Where do they want help and guidance on AI?"

How will you create safeguards to reduce the risk of plagiarizing from published material?

What consequences will result from intentional or unintentional violations of the policy. What responsibilities do team members have to report suspected violations?

How should they report them?

What will happen if someone made an honest mistake in their use of AI?

What if someone intentionally misled others about their use of AI, or used it in a malicious way?

Get Your Team's Support

Once you've outlined what you want an AI policy to cover, ask your team for their input. How do team members feel about AI use? Where do they want help and guidance on AI? Their answers will help you build a custom policy to guide how your team informs and educates itself and its community. And once you have a draft policy, get feedback before you roll it out.

A logical next question for many teams: Can we use AI to write our AI policy? Sure—with caveats.

- Does having AI draft or assist with drafting your policy fit the values and approach your team has identified for your AI use?
- Would a team member using AI to draft a policy from scratch fit with how your leadership wants your team to use this technology?
  - If yes, use thoughtful, specific prompts to ask an approved AI tool to create a draft policy that meets your needs.
  - If no, consider how you might use AI to assist in creating a policy in ways that meet your nonprofit's values.
- Could your team do its own rough draft and prompt AI to draft elements or provisions that stumped you?
- Could you do a rough draft with no confidential information and feed it into an AI tool—ideally an enterprise one—to ask it what areas you might have missed or could strengthen?

Remember: Presumably, your nonprofit wants to use AI to augment and support your work, not replace critical thinking. If your team has decided an AI policy is important, make human review at the beginning and end a priority, and keep all the actual decision-making with humans.

Making It Happen

Here are some concrete next steps you can use to help your policy become reality.

1. **Form a small AI policy team**
   - Involve a handful of people from key areas of your organization—

CONTINUED ON NEXT PAGE

How to Create a Nonprofit AI Policy

CONTINUED FROM PAGE 10

programs, communications, operations, development, HR, IT.
- Consider appointing a key player or two, then asking for volunteers.

2. Do an AI inventory

- Conduct a brief anonymous survey: What tools do people use now? For what purpose? With what data?
- Evaluate what you learn about existing AI use for risks and prioritize policy elements accordingly.

3. Create a first draft

- Focus on basic components: Purpose, Acceptable/Prohibited Uses, Data Privacy, Governance, Training/ Review. You can add nuance later.
- Aim for good, not perfect!

4. Share and train

- Hold a short all-staff briefing and share one-page "Do / Don't" guidance.
- Reinforce and discuss the policy at onboarding and manager check-ins with team members.

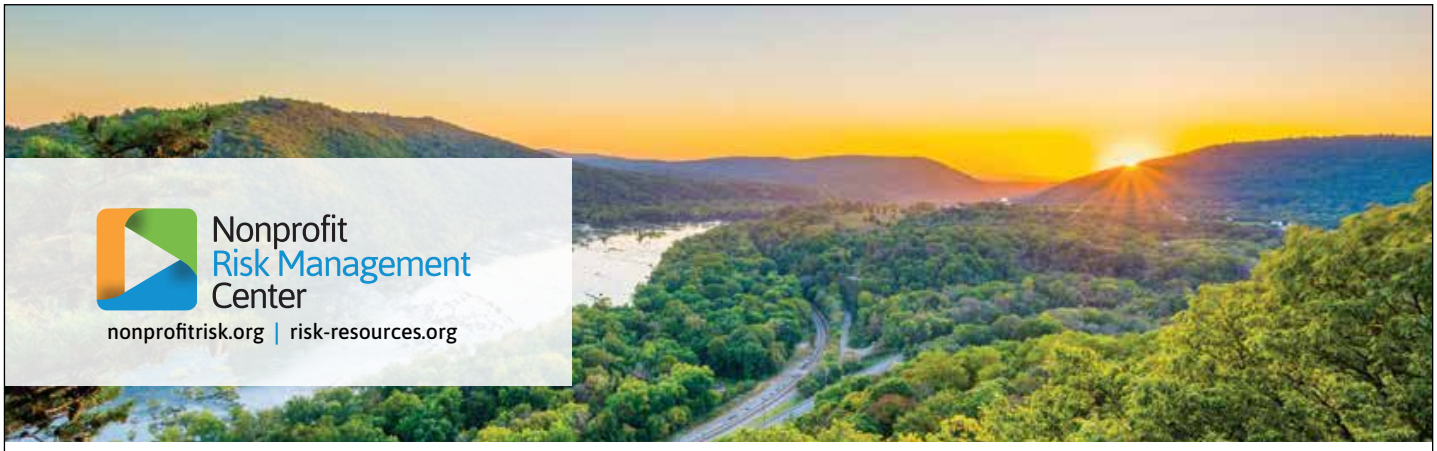
5. Review and evolve

- Create a policy review schedule (e.g., 6–12 months) to incorporate lessons learned and new requirements from regulators, funders, or other parties.
- Build in processes for feedback from staff and, ideally, your community.

Stay Flexible

Once you establish your AI policy, revisit it regularly. You may need to make changes and additions as you uncover new challenges and benefits of AI use. A simple, flexible structure will provide a consistent backbone for your work with AI as technology rapidly evolves. Your team has learned lots of new things together and navigated complex issues. Draw on that knowledge to help you shape a policy to navigate AI. You've got this.

Rachel Sams is Lead Consultant and Editor at the Nonprofit Risk Management Center. She holds an AI for Nonprofits certificate from NTEN and has spent the past several years curious, concerned, and in learning mode on AI risk for nonprofits. Reach her with thoughts or questions about this article at rachel@nonprofitrisk.org or (505) 456-4045.



FIND THE ANSWERS HERE

Inspiring effective risk management and Risk Champions across the diverse nonprofit sector.

Consulting Services

Engagements tailored to help you advance risk management for your mission

Affiliate Membership

Exclusive resources to build your risk expertise, policies, and plans

HR & Risk Resources

Free, practical HR and risk resources at risk-resources.org

RISK eNews

A quick-read newsletter with tangible risk tips specifically for nonprofits

RME Magazine

An in-depth look at nonprofit risk topics published three times a year

Call Us: (703) 777-3504

www.nonprofitrisk.org | 204 S. King Street, Leesburg, VA 20175 | info@nonprofitrisk.org

Do You Know Where Your Data Is—And How To Protect It?

By Elyzabeth Joy Holford

All nonprofits—from local community organizations to international foundations—operate as data repositories. Every day, your team holds the keys to sensitive information, including data such as donor names, financial details, employee records, and beneficiary personal data. For cybercriminals, this information is not just data; it is currency.

We live in an era in which cyberattacks on nonprofits are not just possible, they are likely. Phishing threats and AI-driven scams have proliferated and working with third-party vendors grows ever more complex. To fulfill your mission, you must protect your organization, your team, and your constituents. A data breach can cost more than money; it can destroy the trust you've spent years building with constituents.

This article focuses on the most important factor in your cybersecurity arsenal: your organizational culture. We've also included some additional, practical steps to securely maintain your data.

Establish and Maintain a Healthy Cyber Culture

Nonprofits often talk about cybersecurity as if it is only an IT challenge, best solved by deploying technology like firewalls and encryption. Yet human error is responsible for a staggering majority of data breaches. This means that our most valuable source of strength—our people—can also be a critical source of vulnerability. A robust, sustainable cybersecurity strategy must be grounded in a "no blame" attitude that fosters acceptance, curiosity, and transparency. This allows employees to help shape the cyber health of an organization through participation. Creating an open, responsive culture requires a deliberate, thoughtful approach. How?

- **Lead by Example and Foster a Speak Up Culture:** Leaders should explicitly state that honest mistakes will not be punished and encourage employees to report issues immediately. Leaders should model vulnerability by openly discussing security challenges and acknowledging their own near misses.
- **Implement Non-Punitive Reporting Mechanisms:** Create simple, anonymous, and accessible channels to report suspicious behavior or accidental clicks, such as a "Phish Alert" button.

CONTINUED ON PAGE 14

Do You Know Where Your Data Is—And How To Protect It?

CONTINUED FROM PAGE 13

> "The first step is to conduct a data inventory, mapping out exactly what data you collect and where it is stored."

- **Turn Mistakes into Learning Moments:** When incidents happen, conduct "post-mortem" or blameless post-incident reviews focused on identifying root causes of the system failure, not assigning blame. These incidents can be transformed into anonymous case studies to educate the whole organization.
- **Recruit Security Champions:** Enlist and empower individuals who are not in IT but can advocate for good practices and act as liaisons.

Assess Where Your Data Lives (Data Inventory)

You cannot protect what you do not know you have. The first step is to conduct a data inventory, mapping out exactly what data you collect and where it is stored. This should cover:

- **Donor Databases:** Your constituent relationship management (CRM) system contains sensitive data about individuals including personal contact information, donation history, credit card data, and bank transfer information.
- **Email Platforms:** These systems often hold internal and external correspondence that may include sensitive conversations.
- **Third-Party Tools:** The event software, online donation portals, and cloud storage providers you contract with will likely have access to multiple data points in your cyber ecosystem.
- **Unstructured Data:** It is easy to forget that the spreadsheets and tables you have on laptops, USB drives, and as attachments in email inboxes often contain very sensitive data.
- **AI Tools:** Whether you have an AI policy or not, your staff may be using AI tools that are not secured.
- **Ghost Data:** There could be lingering copies of data in the backups, snapshots, and cloud storage logs that you use. This data consumes storage space, which costs money. It can also contain sensitive information which,

CONTINUED ON NEXT PAGE

Do You Know Where Your Data Is—And How To Protect It?

CONTINUED FROM PAGE 14

if left unprotected, presents another target for gaining access to your systems.

Identify Your Vulnerabilities

Once you know where your data lives, assess how it could be compromised. The primary areas to investigate include:

- **Human Error:** Even in a risk-aware organization, it is important to keep your team vigilant to the fact that bad actors will try to promulgate scams. Phishing emails are becoming increasingly personalized, using AI to mimic the words and voices of donors, staff, board members, or executive directors.
- **Weak Authentication:** Using simple passwords or failing to use multi-factor authentication (MFA) for entry into databases makes it easier for cybercriminals to access your systems.
- **Third-Party Vendors:** If a vendor such as your online donation processor or your cloud service provider is compromised, your data is compromised.
- **Insecure AI Use:** One of the most common AI use errors is accidentally pasting information from employee and/or donor lists into unauthorized AI tools, which can expose confidential information.
- **Remote Work/Unsecured Networks:** Your data can be exposed to attack when staff access sensitive systems over public WiFi or from unpatched devices.

Take Steps to Protect Your Data

Protecting your organization from cyberattacks is not about perfection; instead, it's about preparedness. Take these important steps:

- **Implement Multi-Factor Authentication (MFA):** MFA is the single most effective technology-based security measure. It requires users to verify their identity via two or more methods, blocking most automated attacks. Enable it for all email, financial, and donor databases.

CONTINUED ON PAGE 16

> "Once you know where your data lives, assess how it could be compromised."

Do You Know Where Your Data Is—And How To Protect It?

CONTINUED FROM PAGE 15

"If you accept any kind of payments online, it is your responsibility to protect those transactions."

- **Gamify and Personalize Training:** Replace long trainings with short, relevant learning modules that use storytelling to illustrate the real-world impact of a single click. Encourage attendees to ask questions. Reward proactive behaviors, such as reporting phishing attempts, rather than only punishing failures.
- **Utilize Penetration (Pen) Testing:** Pen tests are proactive, authorized cybersecurity exercises where security professionals simulate real-world attacks to identify, exploit, and remediate vulnerabilities in IT infrastructure, applications, and networks. Pen tests can simulate external attacks on internet-facing assets like websites and servers, or malicious insider or compromised employee activities.
- **Limit Access and User Roles:** Not every employee needs access to all donor data. Implement role-based access control, also known as the principle of least privilege. Ensure that staff only have access to data needed for their positions.
- **Secure Your Payments:** If you accept any kind of payments online, it is your responsibility to protect those transactions.
- **Avoid the Storage of Sensitive Data:** Do not ask for credit card numbers via email and never store CVV numbers or full magnetic stripe data. The better practice is to use reputable payment processors or specialized donor platforms that are PCI-compliant, meaning they follow the strict data security requirements found in the Payment Card Industry Data Security Standard (PCI DSS).
- **Back Up Data:** Many organizations adopt the "3-2-1" rule: maintain 3 copies of data, on 2 different mediums, with 1 copy offsite/cloud. Some organizations rely on automated cloud-based backups and external hard drives. It is important to have a plan to back up data and make sure that plan is followed across the organization.
- **Purge and Archive:** If you don't need it, delete it. A data retention policy can set the cadence for safely destroying old records.
- **Encrypt Everything:** Ensure all laptops are encrypted and your website uses Hypertext Transfer Protocol Secure (HTTPS) to protect data in transit. Using HTTPS means encrypting the connection between a user's browser and your website using SSL/TLS protocols, protecting data in transit from eavesdroppers and cybercriminals.
- **Develop a Cyber Incident Response Plan:** If a breach occurs, you need a plan to act quickly. Your plan should document exactly who does what in the first 24–72 hours, including providing guidance on when and how to contact law enforcement, legal counsel, your insurance agent, your staff, affected donors, and other appropriate constituents.

Data as Mission Enabler

In the end, cybersecurity isn't just about protecting systems or preventing unflattering headlines. It's about encouraging your team to be more security-minded in an increasingly volatile digital world. By creating a supportive environment, taking inventory of your data, recognizing your vulnerabilities, and implementing robust, proactive security measures, you can protect your data from digital threats and clear the path to successfully achieve your mission.

Elyzabeth Joy Holford is Assistant Executive Director at the Nonprofit Risk Management Center. Reach her with thoughts or questions about this article at elyzabeth@nonprofitrisk.org or (703) 777-3504.

Data Safety Tools

As noted elsewhere in this edition of *Risk Management Essentials*, cybersecurity is never just about firewalls and checklists; it requires an organizational commitment to talk openly and transparently about the opportunities and challenges of your team's data-handling practices. However, part of good data hygiene is having tools to do the job. This checklist, reminder list, and emergency reporting protocol are designed to provide another layer of safety for your data by helping your team spot and report potential "silent" data leaks in their daily habits.

The "Human Firewall" Data Safety Checklist

1. Email & Communication

- ❑ Check the "To" field twice: Auto-complete often suggests the wrong person or wrong address. Before hitting send on an email with sensitive info, did I verify the recipient's address?
- ❑ Review for Personally Identifiable Information (PII) in plain text: Did I avoid putting Social Security numbers, credit card details, or sensitive health information directly in the body of an email?
- ❑ Keep internal matters internal: Am I using encrypted internal tools (like Slack or Teams) for sensitive chats instead of my personal SMS or WhatsApp?

2. File Management & Storage

- ❑ Check the file access status: When working with cloud folders (Google Drive/SharePoint), do I have the access set to "Restricted" or "Only people in my organization" rather than "Anyone with the link"?
- ❑ Clean up downloads: Did I delete sensitive reports or donor lists from my computer's "Downloads" folder once I finished uploading them?
- ❑ Avoid using "Shadow IT": Am I strictly using the organization's approved software, rather than personal accounts or unapproved "free" apps to move data?

3. Remote & Office Habits

- ❑ The Multi-Factor Authentication (MFA) Rule: Is MFA active on every work account I use, especially on my phone?
- ❑ Lock it up: Do I lock my computer screen (Win+L or Cmd+Ctrl+Q) every single time I step away from my desk, even for a coffee?
- ❑ Physical paper trail: Are donor checks, printed reports, signup sheets or other hard copy documents stored in a locked drawer rather than sitting on top of my desk?

4. Device Security

- ❑ Pay attention to public Wi-Fi use: Public Wi-Fi is a playground for data sniffers. If I'm working from a cafe, am I using the organization's VPN?
- ❑ Respond to update prompts: Updates often contain critical security patches for known leaks. Did I click "Install" on that software update today?
- ❑ Follow lost device protocol: Do I know exactly who to call if my work phone or laptop is lost or stolen?

CONTINUED ON PAGE 18

Data Safety Tools (continued)

Red Flag Reminders

If you notice any of the following, report it to IT/Management immediately:

- ❑ A "password reset" email you didn't request.
- ❑ A colleague asking for sensitive info via a new or "personal" email address.
- ❑ An unexpected pop-up asking you to "re-verify" your login credentials.

Emergency Reporting Protocol: What to Do if You Spot a Leak

If you suspect data has been compromised, lost, or accidentally shared, time is your most important asset. Do not wait to be sure that there is a problem—report what you suspect as soon as possible.

Step 1: The Immediate Notification

- ❑ **Primary Contact:** [Insert Name/Title, e.g., IT Manager or Director of Operations]
- ❑ **Phone/Extension:** [Insert Number]
- ❑ **Email:** [Insert that person's email or the Dedicated Security Email if your team has one, e.g., security@nonprofit.org]
- ❑ **Backup Contact:** [Insert Executive Director or Board Member Name]

Step 2: Contain the Breach

- ❑ **Do Not Delete:** If you received a suspicious email or file, do not delete it until IT has seen it. They may need it for forensics.
- ❑ **Disconnect (If Necessary):** If your computer is behaving strangely (files moving, windows opening), disconnect from the Wi-Fi or unplug the ethernet cable immediately.
- ❑ **Change Your Password:** If you think your credentials were stolen, change your password from a different, secure device and alert your supervisor so they can reset your account tokens.

Step 3: Document the Details

While the event is fresh, quickly note down:

- ❑ **What happened?** (e.g., "I clicked a link," "I lost my laptop," "I sent a donor list to the wrong person.")
- ❑ **When did it happen?** (Date and approximate time).
- ❑ **What data was involved?** (e.g., Names, credit card digits, addresses, or medical records).

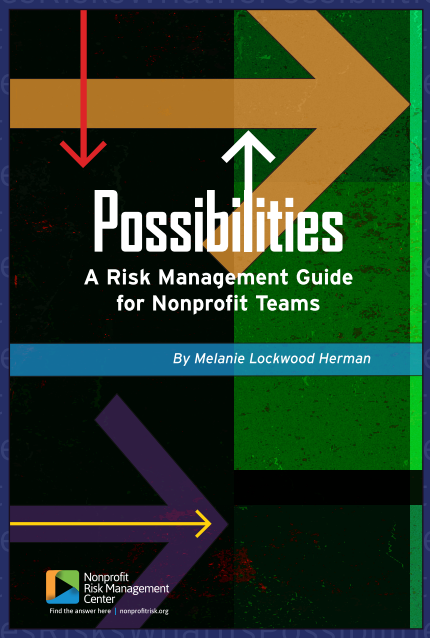
Step 4: Avoid Public Discussion

- ❑ **Internal Only:** Do not discuss the potential leak on social media or with external partners until the leadership team has provided an official statement. This protects the organization's legal standing and donor trust.

Your Risk Reading List Starts Here

NRMC's Newest Publication: *Possibilities*

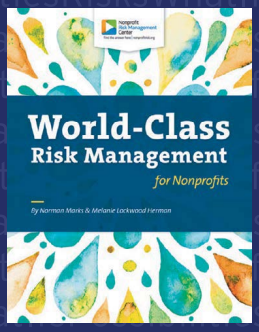
The NRMC team believes risks are simply possibilities: no more, no less. And you can take steps to understand, evaluate, and prepare for a possibility—even, and especially, when you don't know exactly how the possibility will play out. That's why NRMC Executive Director Melanie Herman has written *Possibilities: A Risk Management Guide for Nonprofit Teams*.

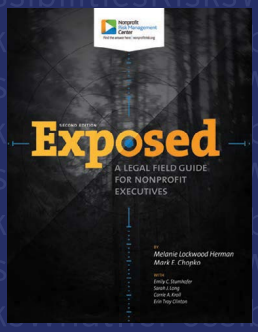


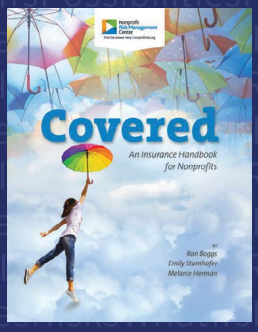
- **Non-member price:** $40
- **NRMC Affiliate Member price:** $36
- **Bulk orders of 10 copies or more:** $32 each

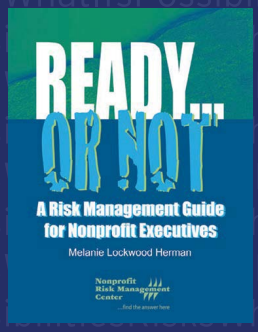
Available in paperback or ePub format

NRMC Favorites Available in eBook Format









Visit www.nonprofitrisk.org/products to purchase these titles and many others on niche risk management topics for nonprofits.

Nonprofit Risk Management Center
Find the answer here | nonprofitrisk.org

FIND THE ANSWER HERE | NONPROFITRISK.ORG
204 South King Street, Leesburg, VA 20175 Phone: 703.777.3504

Nonprofit Risk Management Center

204 South King Street
Leesburg, VA 20175

Risk Management ESSENTIALS

Tips, Knowledge and Tools for Nonprofit Organizations

PLEASE ROUTE TO:

- ☐ **Executive Director**
- ☐ **Director of Volunteers**
- ☐ **Risk Manager**
- ☐ **Legal Counsel**
- ☐ **Human Resources**
- ☐ **Finance/Administration**

NEW AFFILIATE MEMBERS

Learn more about NRMC's Affiliate Member program at nonprofitrisk.org/affiliate-membership. NRMC would like to welcome our new Affiliate Members.

Episcopal Relief & Development

LCMS Foundation

INSIDE THIS ISSUE