



START HERE: NONPROFIT CYBERSECURITY BASICS

**A Companion to the Community IT
Innovators Cybersecurity Playbook**



Why This Guide

You know you should be doing something about cybersecurity. Maybe you're the accidental techie, the person who ended up owning IT because someone had to. Or you're an Executive Director or board member trying to figure out where your organization actually stands. You don't need to have a security background to manage cybersecurity, and our full Cybersecurity Playbook can feel like a lot to take in at once.

This guide is a short companion to the Playbook. It's a path through the first level, what we call Foundational. It's written for someone starting from scratch or trying to figure out what to tackle first. Think of it as the on-ramp. When you're ready for more detail on any topic, the full Playbook is there. That's true whether you're a four-person nonprofit or a forty-person one. Small, consistent changes add up to real protection. A risk assessment can help you figure out where to invest first, but you don't need one to begin.

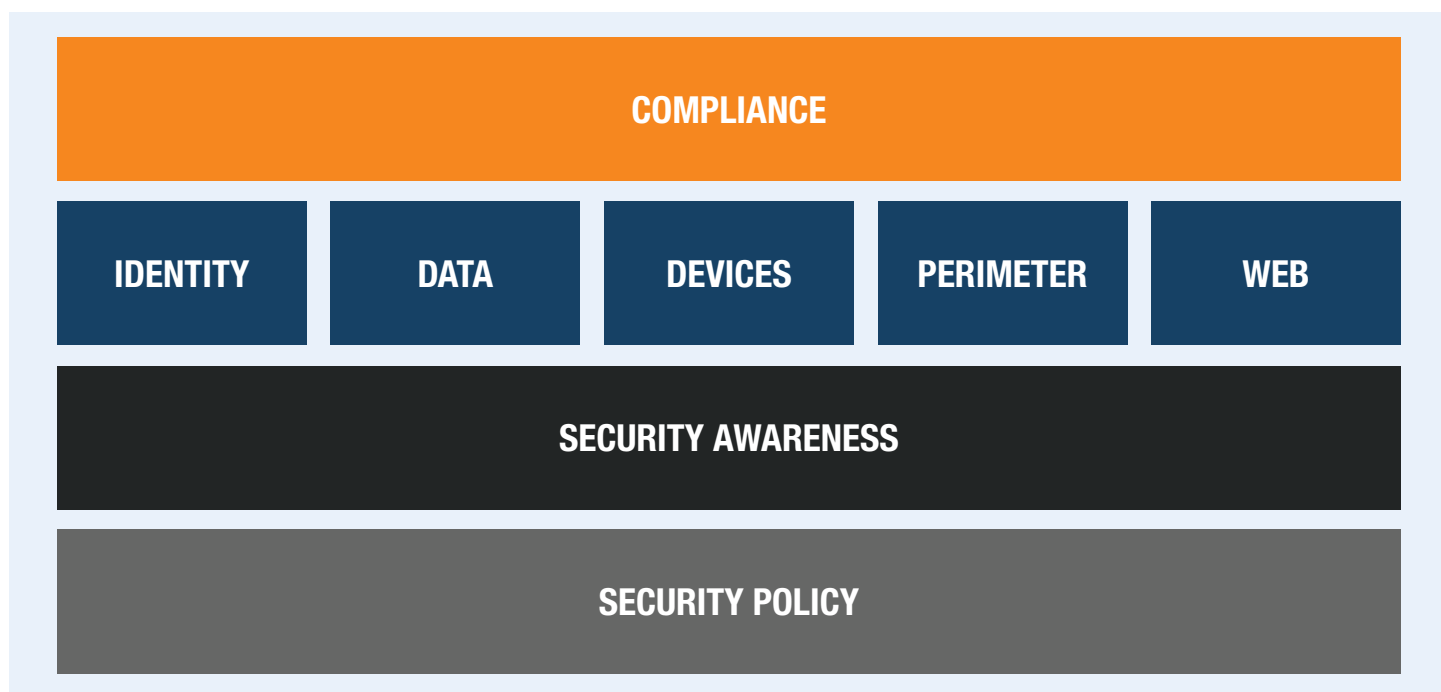
You don't need a perfect plan. You need to start.

None of the steps in this guide should cost your organization an arm or a leg. What matters is putting them in place together. Cybersecurity is a journey not a destination. The value of this path isn't in any single step; it's in steady incremental progress that builds on a strong foundation. A password manager alone helps. A password manager, MFA for all staff and passkeys for financial staff, and the ongoing training to use them correctly? That's an even stronger security posture.

How We Think About Cybersecurity

We organize cybersecurity into four layers, and we use this same framework in our webinars and throughout the Playbook:

- ⦿ **Policy** is the foundation: the decisions your organization has made about how to handle data, devices, and access.
- ⦿ **Training** is your people: the most effective, and most overlooked, line of defense.
- ⦿ **Technical** is the layer most people think of first: identity, data, devices, perimeter, and web protections. It matters, but it's not where you should start.
- ⦿ **Compliance** caps the whole thing: it offers a defined set of requirements to follow and lets you check that the other three layers are being followed.



A quick note on AI: it's changed the threat landscape. Attackers use it, of course, and it can also create new risks through how your own staff use it. It can also help you close security gaps when implemented intentionally. AI literacy is vital whether your nonprofit chooses to use AI or decides not to. This guide focuses on the fundamentals that matter more than ever in the age of AI but does not require or advocate for the use of AI.

1 Own It

Before anything else: decide who owns this.

Sit down with your team and make cybersecurity part of someone's actual job description or portfolio, not a task that floats around and lands on whoever noticed the problem most recently. This owner doesn't need to have a technical background. What they need is the authority to prioritize cybersecurity, ask the right questions, hire the right people and vendors, and advocate for training, budget, and policy.

This step matters more than anything else in this guide. Without a named owner, cybersecurity stays reactive.

You're forever the accidental techie, fixing what breaks. With clear ownership, your organization moves into a strategic posture: someone is watching the whole picture, not just today's fire. That shift makes everything else in this guide easier to act on.

This applies to nonprofits at every size. The person doesn't necessarily need a security title; they need the standing to make the case.



2 Do This First, Then Close the Gaps

Four moves block the #1 way attackers get in.

Once someone owns cybersecurity at your organization, here's the order we'd tackle things in, highest-impact first.

DO THIS FIRST

Multi-Factor Authentication (MFA) Adds a second check beyond your password, usually your phone or a security key. Most breaches start with a compromised account; MFA is the single most effective thing you can do to stop that. Where you can, prioritize staff with access to sensitive systems like Finance, IT, HR first. Where possible, use a phish-resistant passkey for these roles and for your entire staff if you can.

Password Manager Every account should have a unique, complex password. A password manager makes that realistic without anyone having to remember them all. There are many reputable low-cost and free versions available.

Security Awareness Training Most attacks start with a malicious email. Regular, ongoing training for staff to spot and resist phishing is one of the best returns on investment available to you. There are several vendors to choose from at affordable subscription levels.

Spam Filtering The most common security issue reported to IT help desks is spam. An effective filter cuts down what your staff has to make a judgment call on.

CLOSE THE GAPS

Patching / Updates Out-of-date software is the source of a majority of breaches. A reliable, verified process for updating operating systems, third-party apps and your organization's website closes this gap.

Antivirus Not perfect on its own, but still a necessary layer, and modern tools increasingly catch what older ones miss.

Backups If something is deleted, corrupted, or held for ransom, you need a way to get it back. Your cloud provider's built-in protection exists to protect them, not you, so make sure you have a real third-party backup from a reputable vendor.

3 Put It in Writing

Five policies turn good habits into standard practice.

Policy work is easy to put off for a day when you have the time. But without it, you're relying on everyone independently doing the right thing, and eventually, someone won't.

- ① **IT Acceptable Use Policy** This is the one to write first, even in simple form. Without it, you will find unacceptable things on your organization's devices. Should cover passwords, a basic information systems inventory, and how work and personal devices are handled. Plenty of templates exist online to adapt.
- ② **Data Privacy Policy** Covers how you handle the data of the people you serve and the people who fund you, including any formal compliance requirements like HIPAA or GDPR that apply to your organization.
- ③ **Data Retention Policy** One of the easiest cybersecurity wins available. Decide how long to keep old files, emails, and communications then delete the rest. Your data can be a liability as well as an asset. Be clear on what data you need to keep and what should be purged. Old data you no longer need is a risk: it's something an attacker can find if they get in, and something AI tools (yours or theirs) can now surface and search far more easily than before. If it's not there to be found, it can't be exposed.
- ④ **AI Acceptable Use Policy** Your staff are likely already using free AI tools, whether you have a policy or not. Decide as an organization which tools are approved and what data can (and can't) go into them. If your policy is that your organization doesn't use AI, put that in writing and share with staff.
- ⑤ **Cyber Insurance** Often comes up naturally once your other policies exist, since insurers increasingly ask what's in place. Find a broker who understands both cyber coverage and nonprofit operations.

A more technical note: if you manage your own email domain, ask whoever handles your IT to check your DMARC/DKIM setup. It's a low-cost way to help prevent your domain from being spoofed. It's covered in more detail in the full Playbook.

4 Close the Loop: Compliance

Turn policy into practice, on a schedule.

None of this works if it just sits on a shelf. This is where the owner from the first step comes back in.

- ⦿ **Make a cybersecurity implementation plan, operationalize it, and use it!** Give your owner concrete milestones not just “own cybersecurity,” but specific steps, dates, and KPIs, so there’s a way to check whether the organization is actually following through, not just whether the policies exist on paper.

Compliance isn’t a separate, technical thing that happens to you. It’s the follow-through that makes everything else in this guide real.



Your Quick-Reference Checklist

OWN IT

- ☐ Someone has cybersecurity as a named part of their job or portfolio

DO THIS FIRST

- ☐ MFA enabled, prioritized for Finance/IT/HR if rolling out in stages
- ☐ Password manager in use organization-wide
- ☐ Regular security awareness training in place.
- ☐ Spam filtering active

CLOSE THE GAPS

- ☐ Patching/updates process for OS and third-party apps
- ☐ Antivirus/anti-malware managed and maintained
- ☐ Backups stored with a third-party provider

PUT IT IN WRITING

- ☐ IT Acceptable Use Policy
- ☐ AI Acceptable Use Policy
- ☐ Data Privacy Policy
- ☐ Data Retention Policy (old files/communications archived or deleted)
- ☐ Cyber insurance conversation started

CLOSE THE COMPLIANCE LOOP

- ☐ Cybersecurity implementation plan in place, with milestones for the owner

Ready to see where your organization stands?

Contact us to take our free cybersecurity risk assessment a guided survey based on the NIST Cybersecurity Framework. See your organization's unique risk profile and get a report you can act on.

Take The Free Risk Assessment

Have questions, or want to talk through where to start? Let's talk.



Where
technology
meets mission

www.communityit.com

1110 Vermont Ave NW #900

Washington, DC 20005

connect@communityit.com