JPert INC

Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · NONPROFITS

Nonprofit IT Setup Guide: Protecting Donors and Mission Data

How a small nonprofit should set up its computers, email, donor systems and volunteer access so donor trust, client confidentiality and the mission stay protected, on a nonprofit budget. Each step says plainly whether the law **requires** it or official guidance **recommends** it.

By Umair Akhtar, Founder & President, JPert INC

Published November 1, 2026
Last reviewed November 1, 2026
About a 12-minute read

JPert INC
1934 Old Gallows Road, Suite 360, Vienna, VA 22182
703-576-8200 · jpert.com

Free to share. The latest version is always at https://jpert.com/white-papers/nonprofit-it-setup

Scan for the latest version

The short version

- No single federal cybersecurity law covers most nonprofits. Virginia's breach notification law does apply, and so do card-industry rules if you take donations by card.
- Virginia's Consumer Data Protection Act exempts nonprofit organizations, so for most nonprofits the binding rules are the breach law, the card rules, and what your grants, contracts and insurer require.
- The free NIST Cybersecurity Framework 2.0 and its Small Business Quick-Start Guide, which NIST says can also help nonprofits, are the best official playbook. Its first function, Govern, is a board responsibility.
- The cheapest secure donation setup keeps card numbers entirely with your payment processor, never on your own systems.

Who this is for and how to read it

This white paper is for executive directors, operations and finance staff, and board members of nonprofits with roughly 5 to 100 staff (plus volunteers) and no full-time IT department. Every recommendation is labeled:

- **REQUIRED** A law or binding industry rule requires it today.
- **RECOMMENDED** Official guidance from NIST, CISA or the FTC recommends it.

This is general guidance, not legal advice. If your nonprofit provides health services, handles student records or works under government contracts, other rules may apply; ask counsel.

The rules that apply today

Virginia's breach law

REQUIRED Virginia's breach notification law (Va. Code 18.2-186.6) applies to organizations that hold residents' personal information, such as Social Security, driver's license or financial account numbers. Nonprofits often hold this data for staff payroll, volunteers' background checks and some donor and client records. If it is exposed unencrypted, you must notify affected residents and the Attorney General without unreasonable delay. Virginia also restricts how Social Security numbers may be displayed, mailed or used (Va. Code 59.1-443.2).

Virginia's privacy law does not apply to nonprofits

The Virginia Consumer Data Protection Act exempts nonprofit organizations outright (Va. Code 59.1-576). You still owe donors what your own privacy policy promises.

Card donations: PCI DSS

REQUIRED If you accept card donations, your agreement with your payment processor binds you to the Payment Card Industry Data Security Standard (PCI DSS). Version 4.x is now in force, and its "future-dated" requirements became mandatory on March 31, 2025. The simplest way to keep your obligations small is to use a hosted donation page or payment form from your processor so card numbers never touch your website, email, spreadsheets or phones. Ask your processor which self-assessment questionnaire applies to you and complete it each year.

Grants, contracts and insurers

Government grants and contracts, foundation agreements and cyber insurance policies increasingly include security requirements, such as MFA or backups, as conditions. Read them; they may be your most specific rules.

Step 1: Govern: make security a board-level habit

RECOMMENDED NIST's Cybersecurity Framework 2.0 added a sixth function, Govern, in February 2024. Its small-business guide starts by asking leaders to understand which

laws, contracts and insurance terms apply, assign responsibility, and budget for security. For a nonprofit, that means:

- Name one staff member responsible for technology risk, supported by your IT provider.
- Give the board a short yearly update: what data you hold, what could go wrong, what you have done, and what it would cost to do more.
- Keep a simple list of what sensitive data you hold (donor, client, staff, payment), where it lives and who can see it. Collect less, and delete what you no longer need.

Step 2: Accounts for staff, volunteers and board members

- RECOMMENDED **Multi-factor sign-in (MFA) on email, remote access, cloud apps and every admin account.** CISA's ransomware guide asks for phishing-resistant MFA on all services, starting with email and remote access. Prefer an authenticator app, passkey or security key over text messages.
- RECOMMENDED **Long passphrases and a password manager.** Current NIST guidance (SP 800-63B, Revision 4) says passwords used alone should be at least 15 characters, should be checked against lists of leaked passwords, and should not be forced to change on a schedule unless there is a sign they were stolen.
- RECOMMENDED **One login per person and separate admin accounts.** Day-to-day work happens on standard accounts. Only a few people hold administrator rights, on separate logins.
- RECOMMENDED **Access ends on the last day.** When someone leaves, turn off email, remote access, shared passwords and building access the same day.

RECOMMENDED **Volunteers and board members** should get their own accounts with only the access they need, never a shared staff login, and should lose access when their term or project ends. Board members using personal email for sensitive discussions is a common gap; give them organization accounts with MFA.

Step 3: Email, scams and donor trust

- RECOMMENDED **Confirm every new or changed bank detail by phone**, using a number you already have, never one in the email. The FBI's 2025 Internet Crime Report recorded more than $3 billion in business email compromise losses, and Virginia ranked 10th in the country in total cybercrime losses ($476.1 million).
- RECOMMENDED **Watch for fake executive requests** for gift cards or urgent payments, a common scam against nonprofits.
- RECOMMENDED **Publish SPF, DKIM and DMARC records**, as the FTC recommends, so criminals cannot easily send fundraising emails that look like yours. Donors who receive a fake appeal in your name lose trust in the real ones.
- RECOMMENDED **Teach staff to spot phishing** and give them one easy way to report it. CISA's Secure Our World campaign reduces the basics to four steps: strong passwords with a password manager, MFA, recognizing and reporting phishing, and automatic updates.

Step 4: Computers, phones and donated equipment

- RECOMMENDED **Encrypt every laptop and phone** that holds work data, so a lost device is a hardware problem, not a data breach. NIST's small-business guide calls for full-disk encryption on laptops and tablets.
- RECOMMENDED **Turn on automatic updates**, and patch internet-facing systems and anything on CISA's Known Exploited Vulnerabilities list first.
- RECOMMENDED **Replace unsupported systems.** Windows 10 support ended October 14, 2025. Machines that cannot upgrade yet need Microsoft's paid Extended Security Updates, which are only available for a limited time, and should be replaced.
- RECOMMENDED **Endpoint protection that someone actually watches**, on every computer. Alerts that nobody reviews do not stop an attack.

RECOMMENDED Donated or personal computers are common in nonprofits. Before one is used for donor or client data, it should be on a supported operating system, encrypted,

updated and protected like any other work computer. Wipe it securely when it leaves.

Step 5: Office network and Wi-Fi

- RECOMMENDED **Separate networks** for staff computers, guest Wi-Fi, and printers, cameras and other smart devices. CISA calls for network segmentation and a current diagram of how data moves.
- RECOMMENDED **WPA3 Wi-Fi** where your equipment supports it, with a long passphrase that changes when staff leave. Guests get internet access only.
- RECOMMENDED **No remote desktop open to the internet.** CISA says remote desktop should never be exposed directly. Use a VPN or secure remote-access service with MFA.
- RECOMMENDED **A supported business firewall**, kept updated and replaced when the manufacturer stops supporting it.

Many nonprofits host visitors, clients or events. Guests should never share the network your staff and donor database use.

Step 6: Backups, cloud services and vendors

- RECOMMENDED **Offline, encrypted, tested backups.** CISA's guidance is to keep offline, encrypted backups of critical data and regularly test them. Many offices follow the "3-2-1" practice (three copies, two types of storage, one off-site) to meet it.
- RECOMMENDED **Back up cloud email and files too.** Cloud services keep your data running, but they are not a full backup plan on their own. Check what is covered and for how long.
- RECOMMENDED **Test a restore** on a schedule and write down how long it took.

RECOMMENDED **Donor databases and fundraising platforms** are vendors too. Check how each one protects your data, whether it supports MFA, and how you would export your data if you left.

RECOMMENDED In 2022, CISA, the NSA, the FBI and allied agencies published joint guidance for organizations that use a managed service provider (MSP). It says your contract should require MFA on every account the provider uses, least-privilege access, defined incident reporting, backup and incident-response duties, and prompt removal of the provider's access when the contract ends. Ask any IT provider, including us, to show you those terms in writing.

Budget note: Microsoft changed its nonprofit program in 2025 and ended the free Business Premium grant; discounted and free tiers remain, and other providers have their own nonprofit programs. Check current eligibility and pricing directly with each provider before budgeting.

Step 7: When something goes wrong

- RECOMMENDED **Write a one-page incident plan**: who to call (your IT provider, your cyber insurer, your attorney, your bank), how to disconnect an infected computer, and how to reach staff if email is down. Keep a printed copy, and walk through it once a year. NIST's incident response guidance (SP 800-61, Revision 3, April 2025) is the current federal reference.
- REQUIRED **Know Virginia's breach law.** If unencrypted Social Security, driver's license, passport, military ID or financial account numbers of Virginia residents are exposed, Va. Code 18.2-186.6 requires notice to those residents and the Virginia Attorney General without unreasonable delay. If more than 1,000 people are notified at once, the Attorney General and the national credit bureaus must also be told. The Attorney General can impose a civil penalty of up to $150,000 per breach. Encrypted data is excluded unless the key was also compromised.
- RECOMMENDED **If money moved to a criminal, act in minutes.** Call your bank to request a recall and report it to the FBI at ic3.gov. The FBI says its Recovery Asset Team froze about 58% of the money it tried to recover in 2025 (about $679 million).

Free and low-cost help for nonprofits

- **CISA's High-Risk Communities resources** list free security programs for civil-society organizations that are targeted because of their work.
- **FEMA's Nonprofit Security Grant Program** (FY2025: $274.5 million nationally) lists "cybersecurity measures on real property" as an allowable cost for eligible 501(c)(3) organizations at risk of terrorist attack. Applications go through your State Administrative Agency, so it is not a general IT grant.
- **CISA's free vulnerability scanning** is open to critical infrastructure organizations. Ask CISA whether your organization qualifies.

One-page setup checklist

Area	What to have in place	Status today
Governance	One named owner; yearly board update; list of sensitive data	RECOMMENDED
Card donations	Hosted processor page; yearly PCI self-assessment	REQUIRED (PCI DSS)
Breach readiness	Notice process under Va. Code 18.2-186.6	REQUIRED
MFA	Staff, volunteers, board members, admin accounts	RECOMMENDED
Accounts	No shared logins; access ends when roles end	RECOMMENDED
Payments	Phone call-back before any change to bank details	RECOMMENDED
Email	SPF, DKIM, DMARC; phishing reporting	RECOMMENDED
Devices	Encrypted, updated, monitored; donated devices included	RECOMMENDED
Network	Separate guest Wi-Fi; no exposed remote desktop	RECOMMENDED
Backups	Offline or locked copy; donor platforms included; restores tested	RECOMMENDED

How JPert can help

JPert is a managed IT and cybersecurity company in Vienna, Virginia, near Tysons, and educating nonprofits about technology is part of our mission. We help nonprofits across

Northern Virginia make the most of nonprofit licensing programs and put these basics in place on a realistic budget. Read about IT for nonprofits, try our free Cyber Safety Checklist, or book a free IT assessment.

Related reading from our Chronicles: donor data protection, board cybersecurity responsibilities and free cybersecurity tools for nonprofits.

Sources

Every recommendation above comes from these official sources, checked on November 1, 2026:

- Va. Code 18.2-186.6 (breach of personal information notification)
- Va. Code 59.1-576 (Consumer Data Protection Act scope and exemptions)
- Va. Code 59.1-443.2 (restricted use of Social Security numbers)
- PCI Security Standards Council: Future-dated PCI DSS v4.x requirements
- NIST Cybersecurity Framework 2.0 (CSWP 29)
- NIST SP 1300: Cybersecurity Framework 2.0 Small Business Quick-Start Guide
- CISA: Secure Our World (four steps)
- FTC: Cybersecurity for Small Business
- Microsoft Learn: Microsoft for Nonprofits program updates
- CISA: Cybersecurity resources for high-risk communities
- FEMA: FY2025 Nonprofit Security Grant Program fact sheet
- FBI: 2025 Internet Crime Report
- NIST SP 800-63B Rev. 4: Authentication and passwords
- CISA: #StopRansomware Guide
- CISA, NSA, FBI and allied agencies: Protecting against cyber threats to MSPs and their customers (AA22-131A)
- NIST SP 800-61 Rev. 3: Incident response recommendations (April 2025)
- Microsoft: Windows 10 end of support and Extended Security Updates

This white paper is general information about IT and security practices, not legal advice. Rules change; we review this paper when the underlying rules or guidance change. See our editorial policy.

FAQ

Common questions from nonprofits

Does Virginia's privacy law apply to nonprofits?

No. The Virginia Consumer Data Protection Act exempts nonprofit organizations. Virginia's breach notification law, Va. Code 18.2-186.6, does apply when a nonprofit holds residents' personal information such as Social Security or financial account numbers.

Do nonprofits have to follow PCI rules for online donations?

Yes, if you accept card donations. Your payment processor agreement binds you to PCI DSS, now version 4.x. Using a hosted donation page from your processor, so card numbers never touch your own systems, keeps your obligations as small as possible.

Where should a small nonprofit start?

Turn on multi-factor sign-in for email, require a phone call-back before any change to bank details, keep an offline or locked backup that you test, and give the board a short yearly update on technology risk.

Are there free cybersecurity resources for nonprofits?

Yes. NIST's Cybersecurity Framework 2.0 Small Business Quick-Start Guide is free and NIST says it can help nonprofits. CISA publishes free resources for high-risk civil-society organizations, and eligible nonprofits at risk of terrorist attack can apply for FEMA Nonprofit Security Grants that allow some cybersecurity costs.

Want us to check your setup against this guide? Book a free IT assessment with our Vienna, VA team at jpert.com/contact or call 703-576-8200. We will give you a plain-English list of what to fix first.