JPert INC

Managed IT & Cybersecurity · Northern Virginia

WHITE PAPER · SMALL BUSINESS

Small Business IT Setup Guide: A NIST-Based Blueprint

A plain-English blueprint for setting up a small office's computers, accounts, email, network, backups and vendors, organized around the six functions of NIST's free Cybersecurity Framework 2.0. 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/small-business-it-setup

Scan for the latest version

The short version

- Most small businesses are not covered by a specific federal cybersecurity law. In Virginia, the binding rules are usually the breach notification law, the Social Security number law, card-industry rules if you take cards, and what your contracts and insurer require.
- NIST's free Cybersecurity Framework 2.0 and its Small Business Quick-Start Guide (both February 2024) give the clearest official structure: Govern, Identify, Protect, Detect, Respond and Recover.
- Business email compromise caused more than $3 billion in reported U.S. losses in 2025, far more than reported ransomware losses. A phone call-back before any payment change is the cheapest control you will ever add.
- Windows 10 support ended October 14, 2025. Any business still running it has a known gap to close.

Who this is for and how to read it

This white paper is for owners and office managers of businesses with roughly 5 to 100 people and no full-time IT staff. 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.

If your business is in healthcare, legal, financial services, government contracting, construction or property management, see our industry-specific white papers too. This is general guidance, not legal advice.

The rules that apply today

- REQUIRED **Virginia's breach law** (Va. Code 18.2-186.6) applies to any business holding residents' Social Security, driver's license, passport, military ID or financial

account numbers, including your own employees' payroll records. If unencrypted data is exposed, notify affected residents and the Attorney General without unreasonable delay.

- REQUIRED **Virginia's Social Security number law** (Va. Code 59.1-443.2) restricts displaying, mailing or embedding SSNs.
- REQUIRED **Card payments** bind you to PCI DSS through your processor agreement. Version 4.x is in force, and its future-dated requirements became mandatory March 31, 2025.
- REQUIRED **The FTC Safeguards Rule** (16 CFR Part 314) applies if your business does anything "financial in nature," such as lending, tax preparation or certain advisory work. Ask counsel if you are unsure.
- **Virginia's Consumer Data Protection Act** applies only to businesses that control or process data on at least 100,000 Virginia consumers, or 25,000 consumers plus more than half of revenue from selling data, so most small businesses fall outside it.

Your **contracts and cyber insurance policy** may be your most specific rules. Many insurers now ask about MFA, backups and endpoint protection before they quote.

Step 1: Govern and Identify

RECOMMENDED NIST's Quick-Start Guide begins with understanding your obligations and your assets.

- **Name an owner** for technology risk, even if most of the work is done by an IT provider.
- **List what the law, your contracts and your insurer require** of you, using the section above.
- **Keep an inventory** of every computer, phone, printer, network device, program and cloud service, and what data each one holds. CIS Controls v8.1 Implementation Group 1, a set of 56 essential safeguards for organizations with limited IT staff, starts with exactly this.

Step 2: Protect: accounts and passwords

- 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.

Cloud office suites include free settings that require MFA for everyone and block old sign-in methods that attackers abuse. Microsoft documents this as "security defaults." Turn on your provider's equivalent if you have nothing better.

Step 3: Protect: email and payments

- 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 **Publish SPF, DKIM and DMARC records** for your domain, as the FTC recommends.
- RECOMMENDED **Turn on your email service's filtering** and tag messages from outside the company.

- RECOMMENDED **Train staff** to recognize and report phishing, one of CISA's four Secure Our World steps.

Step 4: Protect: computers, phones and the network

- 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 **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.

Step 5: Detect

RECOMMENDED NIST's Quick-Start Guide asks small businesses to monitor for unusual activity, and advises them to "consider a service provider to monitor networks" if they

lack in-house resources.

- Have endpoint protection alerts and sign-in alerts go to someone who will act on them, including after hours.
- Keep logs from email, firewalls and key systems. CISA recommends keeping critical system logs for at least a year.

Step 6: Respond and Recover

- 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 **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).

Step 7: Vendors and your IT provider

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.

RECOMMENDED For every cloud service that holds business data, know who in your company administers it, whether MFA is on, and how you would get your data out.

One-page setup checklist

Area	What to have in place	Status today
Obligations	List of laws, contracts and insurance terms that apply	RECOMMENDED
Breach readiness	Notice process under Va. Code 18.2-186.6	REQUIRED
Card payments	Processor-hosted payments; yearly PCI self-assessment	REQUIRED (PCI DSS)
Inventory	Every device, program and cloud service	RECOMMENDED
MFA	Email, remote access, cloud apps, admin accounts	RECOMMENDED
Payments	Phone call-back before any bank detail change	RECOMMENDED
Email	SPF, DKIM, DMARC; filtering; phishing reporting	RECOMMENDED
Devices	Encrypted, updated, monitored; no unsupported Windows 10	RECOMMENDED
Network	Separate guest Wi-Fi; no exposed remote desktop; supported firewall	RECOMMENDED
Detect	Alerts reach someone who acts; logs kept a year	RECOMMENDED
Backups	Offline or locked copy; cloud data included; restores tested	RECOMMENDED

How JPert can help

JPert is a managed IT and cybersecurity company in Vienna, Virginia, near Tysons. Our small-office plans include 24/7 security monitoring, backups, patching, security awareness training and a local help desk, which covers most of this blueprint. See plans and pricing, read about IT for small businesses, or book a free IT assessment.

Related reading from our Chronicles: business email compromise prevention, cyber insurance for small business and disaster recovery for small business.

Sources

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

- NIST Cybersecurity Framework 2.0 (CSWP 29)
- NIST SP 1300: Cybersecurity Framework 2.0 Small Business Quick-Start Guide
- NIST SP 1300 (PDF): Small Business Quick-Start Guide
- CIS Controls v8.1 Implementation Group 1
- CISA: Secure Our World (four steps)
- FTC: Cybersecurity for Small Business
- Microsoft Learn: Security defaults in Microsoft Entra ID
- Va. Code 18.2-186.6 (breach of personal information notification)
- Va. Code 59.1-443.2 (restricted use of Social Security numbers)
- Va. Code 59.1-576 (Consumer Data Protection Act scope and exemptions)
- PCI Security Standards Council: Future-dated PCI DSS v4.x requirements
- FTC Safeguards Rule, 16 CFR Part 314 (eCFR)
- 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
- Wi-Fi Alliance: Wi-Fi security and WPA3

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 small businesses

Is there a cybersecurity law that applies to every small business?

Not at the federal level for most businesses. In Virginia, the breach notification law and the Social Security number law apply broadly, card-industry rules apply if you take cards, and the FTC Safeguards Rule applies if your business does anything financial in nature.

What framework should a small business follow?

NIST's Cybersecurity Framework 2.0 and its free Small Business Quick-Start Guide, both published in February 2024. They organize security into six functions: Govern, Identify, Protect, Detect, Respond and Recover.

What are the first three things to do?

Turn on multi-factor sign-in for email and remote access, require a phone call-back before any change to payment or bank details, and keep an offline or locked backup that you test.

Do small businesses still running Windows 10 need to act?

Yes. Windows 10 support ended October 14, 2025. Machines that cannot be upgraded right away need Microsoft's paid Extended Security Updates, which are only available for a limited time, and should be replaced.

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.