

HOUSTON LABS LLC

ZERO TRUST · CIVILIAN FIELD MANUAL

# Zero Trust Phase One: Build Your Foundation

---

Zero Trust implementations for high-risk individuals and small organizations

First Edition · 2026 · Adapted from the NSA Zero Trust Implementation Guideline: Phase One (Jan 2026)

# Contents

---

About This Guide .....	3
How to Use This Guide .....	5
Pillar 1 · You: Accounts & Identity .....	8
Pillar 2 · Your Devices .....	11
Pillar 3 · Apps & Software .....	14
Pillar 4 · Your Data .....	17
Pillar 5 · Network & Environment .....	20
Pillar 6 · Automation .....	23
Pillar 7 · Visibility & Awareness .....	26
Phase One Completion Checklist .....	30
Appendix A: NSA Phase One Crosswalk .....	32
Appendix B: Sources & Acknowledgements .....	33

# About This Guide

---

This guide is the hands-on implementation companion to the Primer. Where the Primer builds your threat model and conceptual framework, this guide tells you what to do: step by step, pillar by pillar, at the foundation level. The emphasis is on execution. You will leave each chapter with a concrete checklist completed, not just a concept understood.

*Phase One: Build Your Foundation* is the first of two implementation guides in this series. It covers the seven Zero Trust pillars at the level of establishing a genuinely secure baseline. No enterprise IT department, no government security team, no unlimited budget. Just you, and possibly a small team, doing the work that makes you meaningfully harder to compromise.

## Who Houston Labs Is

Houston Labs LLC is a technological research and development company, based in New York and established in 2025. We build the tools, systems, and ideas at the frontier where advanced technology meets human creativity, across applied research, creative technology, products and ventures, and advisory and education. Our mission is to further humanity by closing the adoption gap: the widening distance between what advanced technology makes possible and what ordinary people and small organizations can actually use.

This Civilian Zero Trust series is part of our free advisory and education work. The high-risk individuals and small organizations we build for, journalists, activists, researchers, founders, legal professionals, organizers, and others operating under real threat without institutional security behind them, are exactly the people the adoption gap leaves exposed. So we translated government Zero Trust doctrine into steps a capable person can actually execute.

We publish this series independently and vendor-neutrally. We have no financial relationship with any security tool or service named in these pages; our guidance is capability-based, describing what a solution must do so you can choose the one that fits your situation.

## What This Guide Adapts

This guide adapts the *NSA Zero Trust Implementation Guideline: Phase One* (January 2026), a U.S. government work released into the public domain. That document defines 36 Activities and 30 Capabilities organized across seven pillars, collectively aimed at establishing a secure Zero Trust foundation. We have reframed, reordered, and translated that framework for civilian use: personal accounts and devices come first, and organizational considerations are treated as additive guidance rather than the primary frame.

Houston Labs LLC is an independent publisher. This guide is not affiliated with, authorized by, sponsored by, or endorsed by the National Security Agency or any agency or department of the U.S. government. The NSA has not reviewed or approved this publication.

## Disclaimer

This guide is provided "as is," without warranty of any kind, express or implied. It is not legal advice. Threats evolve, tools change, and best practices shift faster than any printed guide can track. Verify current recommendations before acting, especially around software versions, specific configuration settings, and any question with legal implications. For legal risk, consult a qualified attorney or the Electronic Frontier Foundation.

Houston Labs makes no representation that following this guide will prevent any specific attack or outcome. Security is a practice, not a destination, and your results depend on your specific threat environment and how completely you execute each step.

First Edition, 2026.

## Read the Primer First

This guide assumes you have already read the Primer and have a working threat model. The Primer explains why Zero Trust matters for civilians, introduces the seven pillars, and walks you through assessing your own risk level and adversary profile. This guide does not repeat that context. It picks up where the Primer leaves off and tells you what to build.

If you have not read the Primer, stop here and read it first. The steps in this guide will make more sense, and you will make better decisions about which items to prioritize, once you understand the framework underneath them.

# How to Use This Guide

---

Before anything else: you should have already read the Primer. That guide establishes the conceptual foundation, your threat model, and the seven-pillar structure this series is built on. This guide assumes all of that. If you are starting here, go back.

## Where Phase One Sits in the Series

The series has three parts. The Primer is the "what and why." Phase One (this guide) is the foundational setup you actually do, before anything else. Phase Two builds on Phase One by adding integration, advanced controls, and organizational depth. You need Phase One completed before Phase Two will make sense or hold together.

Phase One covers all seven pillars at the level of getting the basics locked in solidly. Each pillar has a defined scope for this phase, and that scope is deliberately tight. The goal is not to do everything possible. The goal is to do the right things first, completely and correctly, so that Phase Two has something real to build on. A partially completed Phase One is not a foundation. It is a liability.

Finish Phase One. Then move to Phase Two.

## The Personal-First Spine

Every pillar in this guide leads with personal implementation: your accounts, your devices, your data, your home network. The steps are written for one person working alone, and that is intentional. Even if you run an organization, your own security posture is the first thing to fix. A compromised account or unencrypted device belonging to the person in charge undoes organizational controls immediately.

Where actions scale to a team or small organization, you will find a clearly marked callout box for that context. Those sections are additive. They do not replace the personal steps; they extend them.


## The Three Callout Boxes

Three types of callout boxes appear throughout this guide. Each one serves a specific purpose. Learn to recognize them.

The **Scaling to your team or organization** box translates the personal steps into organizational actions: what to deploy, what policy to set, what process to establish for a small team. Read these sections if you manage or are responsible for other people's security.

The **If you're being targeted** box appears where the stakes for high-risk individuals are meaningfully higher than the baseline. If you are a journalist covering a sensitive beat, an act-

ivist facing surveillance, or anyone with concrete reason to believe you are already a target, read these sections carefully. They raise the minimum acceptable floor.

The  **Common mistakes** box lists the specific errors that people at this stage routinely make. These are not theoretical edge cases. They are the mistakes that show up repeatedly in post-incident reviews. Read them before you execute the steps, not after.

## The Seven Pillars

This guide is organized by the same seven pillars as the NSA framework and the Primer: User, Device, Apps & Software, Data, Network & Environment, Automation, and Visibility & Awareness. Each chapter covers one pillar and follows a consistent structure:

- Why this pillar matters at this particular phase of your security build.
- Concrete, ordered steps to complete, written for direct execution.
- A checklist you can use to verify your work before moving on.
- Scaling guidance for teams and small organizations.
- Elevated guidance for individuals who are actively targeted.
- Common mistakes specific to this pillar and this phase.

Each chapter ends with a single completion statement: **You're done with this pillar when** followed by a clear, verifiable condition. Treat that line as your exit criterion. Do not move to the next pillar until you can honestly satisfy it.

## How to Work Through This Guide

Work through the pillars in order. They are numbered for a reason. Some steps in later pillars depend on what you configured in earlier ones: your password manager must exist before you can secure every account; your backup must be running before you can meaningfully assess your data risk.

Read each chapter fully before you start executing. The context in the "Why this matters now" section changes how you will approach the steps. Do not skip to the checklist and work backwards.

Set aside real time. Phase One is not something you complete in a single afternoon. Budget several focused sessions across a week or two. Some steps, including firmware updates, backup verification, and account recovery lockdowns, require time to complete and confirm correctly. Rushing them produces the illusion of security without the substance.

A consolidated Phase One Completion Checklist is included at the back of this guide. Use it as your final review once you have worked through all seven pillars, not as a shortcut past the chapters themselves.

When every item on that checklist is done, and you can verify each one, you are ready for Phase Two.

## PILLAR 1 · USER

# You: Accounts & Identity

---

## Why this matters now

Your accounts are the front door. Attackers rarely need to break through your devices or defeat your network if they can walk in using your credentials. The combination of reused passwords and missing second factors is the most consistently exploited weakness across every threat level, from opportunistic credential stuffing to targeted account takeover. Before you touch any other pillar, close this one. Every other layer you build assumes your accounts are not actively compromised.

## Do this

Work through these steps in order. The order matters: get your password manager running before you change passwords, and get your most critical accounts secured before you work outward.

1. **Choose and install a password manager.** Look for one that stores your vault encrypted end-to-end (so the provider cannot read it), supports all your devices, has a browser extension, and has a track record of independent audits. Install the desktop app and the browser extension before you do anything else.
2. **Install the mobile app and link it to your vault.** Enable biometric unlock for convenience, but set a strong master passphrase as the fallback. Write that passphrase down on paper and store it somewhere physically secure. Losing your master passphrase can mean losing access to every account you store.
3. **Add your most critical accounts first.** Start with: your primary email, any secondary email addresses, your bank accounts, credit cards, and your primary work accounts. Generate a new, unique password for each one using the manager's built-in generator. Set length to at least 20 characters. Do not reuse any password.
4. **Work outward from there.** Over the next week, add every other account you use. Any time you log in to a site and realize the password is old or reused, generate a new one immediately. Do not try to do all of this in one sitting.
5. **Enable multi-factor authentication on email first.** Email is the master key. Whoever controls your email controls your account recovery for almost everything else. Use an authenticator app (time-based one-time passwords) rather than SMS. Popular authenticator apps are standalone, work offline, and do not require a phone number.
6. **Enable MFA on financial accounts and primary work accounts.** Apply the same authenticator-app preference. Where a site offers only SMS, that is still better than nothing, but note it as a weak link to upgrade later.



7. **Download your recovery codes.** Every account that issues recovery codes (Google, GitHub, and most authenticator-based accounts do) will show them once, at setup. Download them. Print them or write them down. Store them somewhere physically secure and offline. Not in your cloud drive. Not in a note on your phone. Somewhere you can reach them if you lose your phone and your laptop on the same day.
8. **Lock down account recovery channels.** On your email provider, review the account recovery settings. If a phone number is listed for SMS recovery, consider whether that number is the most secure path or whether it creates a SIM-swap risk. At minimum, make sure no recovery email points to an insecure account. Remove recovery options you do not control.
9. **Audit active sessions.** On your email account and any other primary accounts, find the "active sessions" or "trusted devices" screen. Revoke any device you do not recognize. Do this once now; you will build a habit of doing it periodically in Pillar 7.

- ☐ Password manager installed on all devices, browser extension active.
- ☐ Master passphrase written down and stored offline.
- ☐ Primary email has a unique password and authenticator-app MFA.
- ☐ All financial accounts have unique passwords and MFA enabled.
- ☐ Primary work accounts have unique passwords and MFA enabled.
- ☐ \* Recovery codes downloaded and stored offline for each MFA account.
- ☐ Account recovery settings reviewed; no insecure SMS or email fallback on critical accounts.
- ☐ Active sessions audited; unrecognized devices revoked.

#### SCALING TO YOUR TEAM OR ORGANIZATION

A shared password manager with team vaults is the right tool here. Look for a product that supports team-based access, enforces unique passwords per user (no shared logins for individuals), and lets an administrator audit who has access to what. Onboard your team by giving each person their own seat. Shared credentials for services should live in a shared vault with controlled membership, not in a spreadsheet or a chat message. Require authenticator-app MFA for every team member on the accounts that matter most. Designate a backup administrator so you are not one lost account away from a recovery crisis.

### IF YOU'RE BEING TARGETED

SMS-based MFA is not safe for you. A motivated attacker can SIM-swap your phone number: they call your carrier, claim to be you, and transfer your number to a device they control. At that point your SMS codes and SMS account recovery are theirs. Move to an authenticator app for every account you can. For your highest-value accounts, particularly your primary email, consider a hardware security key. A hardware key is a physical device you tap or insert to prove identity; it is phishing-resistant in a way that one-time codes are not. Also: consider whether your public-facing email address is the same one your accounts are registered to. Separating your contact email from your account recovery email removes one vector.

### ▲ COMMON MISTAKES

- Using SMS as MFA and calling it done. SMS is better than no MFA, but it is a weak second factor. Plan to replace it.
- Installing the password manager on one device only. If that device is lost, stolen, or broken, you are locked out of everything. Install it everywhere.
- Storing recovery codes in the cloud. Recovery codes exist for the scenario where you have lost access to your devices and accounts. Storing them in cloud notes defeats the purpose.
- Using the same master passphrase as an existing account password. Your vault's master passphrase should be unique and strong. It protects everything else.
- Skipping account recovery lockdown. Changing your password and adding MFA while leaving an insecure phone number as your recovery option leaves the back door open.

**You're done with this pillar when:** every critical account has a unique password stored in your manager, your primary email and financial accounts have authenticator-app MFA, recovery codes are stored offline, and you have audited your active sessions and account recovery settings.

## PILLAR 2 · DEVICE

# Your Devices

---

## Why this matters now

A stolen or seized device hands an attacker everything on it and every account session stored on it, unless the data is encrypted and the device is locked. Unpatched software gives attackers a known path in without needing your password at all. This pillar handles the basics that make physical access and unpatched exploits ineffective: encryption at rest, a strong lock, automatic updates, and the ability to wipe remotely. None of this is complex. It is all worth doing before you do anything else at the device layer.

## Do this

- 1. Enable automatic OS updates on every device.** On macOS: System Settings, General, Software Update, turn on "Install updates automatically." On Windows: Settings, Windows Update, turn on automatic updates and "Receive updates for other Microsoft products." On iOS and Android: navigate to the system update settings and enable automatic updates. Do this on every laptop, desktop, phone, and tablet you own before you do anything else on the list.
- 2. Verify encryption is enabled.** On a Mac with Apple silicon or a T2 chip, FileVault encrypts automatically once you set a login password, but confirm it is on: System Settings, Privacy & Security, FileVault. On an Intel Mac without a T2, you may need to turn it on manually. On Windows, check for BitLocker under Control Panel, System and Security, BitLocker Drive Encryption. On Windows Home editions, look for "Device encryption" in Settings, Privacy & Security. On iOS, encryption is on by default once you set a passcode; verify you have a passcode set. On Android, go to Settings, Security, and confirm encryption is enabled; most modern Android devices encrypt automatically when a lock screen is set.
- 3. Set a strong lock on every device.** Laptops and desktops: use a passphrase rather than a short PIN. Aim for at least four random words or a password of 12 or more characters. Phone: use a six-digit PIN at minimum; longer is better. A four-digit PIN has ten thousand combinations; a six-digit PIN has one million. Biometrics (Face ID, fingerprint) are convenient, but the device falls back to the PIN or passphrase when biometrics fail, so the underlying code is what matters. Set the screen lock timeout to no more than two minutes on a laptop; one minute on a phone.
- 4. Enable Find My or Find My Device.** On Apple devices: Settings or System Settings, your Apple ID, Find My. Turn on Find My iPhone or Find My Mac. Confirm "Send Last Location" is on so the device reports its location before the battery dies. On Android: Settings, Google, Find My Device, and verify it is enabled. On Windows: Settings, Privacy & Security, Find My Device. Test that you can see the device at the provider's website before you need it in an emergency.

5. **Confirm remote wipe is available.** On Apple devices, remote wipe is built into Find My. On Android, the same Find My Device panel includes a remote erase option. Know where this is before you need it. If your device stores sensitive data, consider doing a test remote wipe on an old device to see how the process works.
6. **Build a simple device inventory.** A short list in your password manager's notes section, or a plain text file stored in your encrypted cloud, is sufficient for now. For each device, record: the device name, the operating system and current version, whether encryption is confirmed on, and the date you last verified it was patched. This is your baseline. You will use it in the quarterly review you will set up in Pillar 6.
- ☐ Automatic OS updates enabled on every laptop, desktop, phone, and tablet.
  - ☐ Full-disk encryption confirmed on every laptop and desktop.
  - ☐ Encryption confirmed on every phone and tablet (lock screen set).
  - ☐ Strong passphrase set on every laptop; strong PIN (6+ digits) on every phone.
  - ☐ Screen lock timeout set to two minutes or less.
  - ☐ \* Find My or Find My Device enabled and verified on every device.
  - ☐ Remote wipe capability confirmed for every device.
  - ☐ Device inventory created with OS version and encryption status.

#### SCALING TO YOUR TEAM OR ORGANIZATION

At the individual level a manual inventory works. For a team, you need a way to verify that every device meets your standards, not just trust that it does. A lightweight mobile device management tool can enforce encryption, OS update requirements, and lock-screen policy across the team's devices without requiring enterprise infrastructure. Several products target small teams and take an hour to set up. At minimum, run a spreadsheet inventory that each team member updates quarterly, and make someone responsible for following up on machines that fall behind on patches. Remote wipe capability is especially important when team members leave: you need a reliable way to wipe devices that may contain organizational data.

#### IF YOU'RE BEING TARGETED

Standard encryption and a strong PIN cover casual access and opportunistic theft. A motivated adversary with physical access and time has more options. Consider a firmware password or BIOS password on laptops to block booting from external media, which can bypass disk encryption on some configurations. On your most sensitive laptop, disable or tape over ports you do not use (Thunderbolt and FireWire present elevated risk when the machine is on and unlocked). Think about where your devices are when you sleep or cross a border: a device that is powered off is more resistant to certain attacks than one that is merely locked. Consider a dedicated device for your most sensitive work: a machine that holds less data has less to lose.

**▲ COMMON MISTAKES**

- Assuming encryption is on without checking. On Windows Home editions especially, BitLocker may not be enabled by default.
- Setting a long screen lock timeout for convenience. A device left unattended for five minutes in a public space is a device that can be accessed. Two minutes costs almost nothing in practice.
- Using a four-digit PIN on a phone that holds sensitive accounts. Ten thousand combinations is not a serious barrier to someone with motivation and time.
- Never testing remote wipe. If you have never gone through the process, you do not know whether it works on your account, or whether the device needs to be online to receive the command.
- Ignoring the device inventory. Without a baseline, you will not know which devices are out of date, and you will not notice when a device goes missing from your list.

**You're done with this pillar when:** every device has automatic updates on, encryption confirmed, a strong lock set with a short timeout, Find My or remote wipe enabled and verified, and you have a written device inventory with OS version and encryption status for each one.

## PILLAR 3 · APPLICATION &amp; WORKLOAD

# Apps & Software

---

## Why this matters now

Every app you install is an attack surface. It can hold permissions to your camera, microphone, contacts, and location. It can phone home to a server you know nothing about. And if it is not updated, it carries vulnerabilities that are often publicly documented and actively exploited. The goal of this pillar is simple: reduce the number of apps to what you actually use, confirm those apps hold only the permissions they need, and make sure they stay patched automatically. You are not hardening anything exotic here. You are removing the obvious exposure you have already accumulated.

## Do this

1. **List every installed app on each device.** On a Mac, look in Applications. On Windows, use Settings, Apps, Installed apps. On iOS, scroll through your home screens and App Library. On Android, go to Settings, Apps. Write down or screenshot the full list. This step alone is often surprising.
2. **Remove anything you have not opened in 90 days.** If you have not needed it in three months, uninstall it now. You can reinstall later if you find you do need it. Unused apps still receive update pings, still hold permissions, and still represent a potential compromise path. The smaller your installed footprint, the smaller your attack surface.
3. **Review permissions on your most-used apps.** On iOS: Settings, Privacy & Security. On Android: Settings, Privacy, Permission manager. On macOS: System Settings, Privacy & Security. Work through location, microphone, camera, contacts, and calendar for each app. Ask one question per permission: does this app actually need this to do what I use it for? If not, revoke it. Change any "always on" location grants to "while using."
4. **Pay particular attention to apps that have broad access.** Any app with access to your contacts list has a copy of your social graph. Any app with microphone access that you did not explicitly grant for a clear reason is worth reviewing. Any app requesting access to your photos without a function that requires it does not need that access.
5. **Enable automatic app updates on every device.** On iOS: Settings, App Store, turn on App Updates. On Android: Play Store, Settings, Network preferences, Auto-update apps. On macOS: System Settings, General, Software Update, confirm "Install app updates from the App Store" is on. On Windows: enable automatic updates in the Microsoft Store settings, and verify non-Store apps have their own auto-update enabled where possible.
6. **Pick one well-maintained browser as your primary.** You do not need three browsers installed for daily use. Choose one with a consistent security update record and a small extension surface. If you have multiple browsers installed and use them interchangeably, you are

multiplying the number of places credentials can be saved and the number of update cycles you need to stay on top of. Keep one primary browser and remove or stop using the others.

7. **Harden that browser.** First: disable or remove every extension you did not intentionally install and do not actively use. Each extension runs with elevated privileges in your browser. Second: enable HTTPS-Only mode. In Firefox, this is under Settings, Privacy & Security. In Chrome and Edge, it is under the lock icon settings or Privacy and Security settings. Third: find any passwords saved in the browser and migrate them to your password manager, then disable the browser's built-in password saving. Your password manager is the right place for credentials, not the browser.
8. **Check for any apps that update only manually.** Some desktop applications, particularly older utilities and small commercial software, do not auto-update. Flag these in your device inventory. You will add a quarterly update check for them in Pillar 6.

- ☐ Full app list reviewed on every device.
- ☐ Apps not used in 90 days removed.
- ☐ Location, microphone, camera, contacts, and calendar permissions reviewed and trimmed on every device.
- ☐ All "always on" location grants changed to "while using" unless there is a clear reason.
- ☐ Automatic app updates enabled on every device.
- ☐ One primary browser chosen; redundant browsers removed or unused.
- ☐ \* Browser extensions audited; unused ones removed.
- ☐ HTTPS-Only mode enabled in primary browser.
- ☐ Browser-saved passwords migrated to password manager; browser password saving disabled.

#### SCALING TO YOUR TEAM OR ORGANIZATION

Standardizing on a supported browser across the team eliminates a category of variance. Pick one browser, document its required configuration (HTTPS-Only, no unnecessary extensions, passwords in the manager), and communicate it as the team standard. For app permissions, the same principle applies: if your team uses a shared device type, write down which permissions are acceptable for which categories of apps. When you evaluate a new tool, include permissions and update cadence in your criteria. An app that has not shipped a security update in 18 months is a liability regardless of how useful it is.

### IF YOU'RE BEING TARGETED

Permissions trimming is not just tidiness for you: an app with microphone or location access on your device is a potential sensor. Review your most-used apps with that lens. For your browser, separate profiles or separate browsers for different risk contexts reduce the chance that a compromised session bleeds into a sensitive one. Use one profile or browser for general browsing and a separate one for sensitive research or communications; those sessions should not share cookies, logins, or history. Be skeptical of browser extensions from small or unfamiliar developers: extensions with access to all page content can read everything you type into every site.

### ▲ COMMON MISTAKES

- Keeping apps installed "in case you need them." Unused apps are not neutral; they are surface area. Uninstall and reinstall if you ever need them again.
- Granting "always on" location to apps that do not require it. Most apps that ask for location need it only while in use. Blanket always-on grants are almost never necessary.
- Treating browser-saved passwords as a password manager. Browser password storage has historically had weaker protections than a dedicated manager and is tied to a single browser. Migrate them.
- Installing extensions without reading what permissions they request. An extension that requests access to all websites and all your browsing data is not a low-risk add-on.
- Ignoring apps that do not auto-update. If an app requires manual updates, it will drift behind unless you build an explicit process to check it.

**You're done with this pillar when:** every device has a trimmed app list with only apps you actively use, permissions are reviewed and set to minimum necessary, automatic updates are running everywhere, and your primary browser is hardened with HTTPS-Only, no unused extensions, and no stored passwords.



## PILLAR 4 • DATA

# Your Data

---

## Why this matters now

You can recover from almost any security incident if your data is intact and your backups are clean. You cannot recover from ransomware, a failed drive, or an account termination if your data exists in only one place. This pillar has two parts: protecting what you have now, and making sure you can get it back later. You are not building a complete data management system here. You are identifying what matters most, getting it backed up to more than one location, and cleaning up the sharing settings that create unnecessary exposure. That is the foundation everything else builds on.

## Do this

1. **Identify your crown jewels.** These are the files, databases, or records that would cause real harm if lost, altered, or exposed. Examples: your working documents and research, financial records, legal documents, contacts and correspondence, photos you cannot replace, and credentials or keys that are not stored in your password manager. Write a short list. You do not need to categorize everything you own; just identify the subset that matters most. That list drives the rest of this pillar.
2. **Confirm your crown jewels are included in an automated backup.** Check right now: where do these files actually live, and are they being backed up automatically? A file that exists only on your laptop's desktop and nowhere else is one hard drive failure away from being gone. If your most important files are not covered by a backup that runs without you thinking about it, that is the first thing to fix.
3. **Set up the 3-2-1 baseline.** Three copies, two different storage types, one off-site. For most people at Phase One, this looks like: your working copy on your device (1), an automatic cloud sync or cloud backup (2, off-site), and a local external drive or a second cloud service (3). The point is redundancy and physical separation. You are not done if all three copies live on the same desk. Your cloud sync counts as off-site. A second cloud backup account at a different provider also counts. A physical drive kept at a different location counts and is worth having for your most critical data.
4. **Enable automatic backup and confirm it is running.** On macOS, Time Machine to an external drive covers local backup. An additional cloud backup service covers the off-site requirement. On Windows, File History or a cloud backup service covers the same ground. On mobile, confirm iCloud or Google One backup is on and current under each device's backup settings. The key word is automatic: manual backups are backups you will eventually forget to run.

5. **Enable encryption on your cloud storage.** Most major cloud storage providers encrypt data in transit and at rest by default. Confirm this is the case for the services you use. Note the difference: server-side encryption means the provider can access your data; end-to-end encryption means only you can. For now, confirm that at-rest encryption is at minimum enabled. You will address the end-to-end question as a Phase Two decision.
  6. **Audit your shared links.** Open your cloud storage provider (Google Drive, Dropbox, OneDrive, iCloud Drive, or wherever your files live) and find the sharing settings. Look for any file or folder shared as "anyone with the link." This is the setting that means any person who finds or receives that link can open the file, with no authentication required. Revoke these unless they are intentionally public. Change them to "specific people" or remove sharing entirely.
  7. **Review folder-level sharing with named collaborators.** Look at every shared folder and ask: does each person listed still need access? Remove former colleagues, ex-partners, or anyone else who no longer has a reason to be there. Access that is never revoked is access that persists long past its purpose.
  8. **Check your trash and retention settings.** Most cloud providers keep deleted files in a trash or version history for a period of time. Know what that window is for your provider. This is your buffer if you accidentally delete something or if ransomware begins encrypting your synced files and you need to roll back to a clean version. Some providers let you extend this window; consider doing so for your most important folders.
- ☐ Crown jewels identified and written down.
  - ☐ Every crown-jewel file confirmed as covered by an automated backup.
  - ☐ 3-2-1 baseline in place: three copies, two media types, one off-site.
  - ☐ Automatic backup running and verified on every device.
  - ☐ Cloud storage encryption confirmed as enabled.
  - ☐ "All "anyone with the link" shares audited and revoked unless intentionally public.
  - ☐ Shared folders reviewed; access removed for anyone who no longer needs it.
  - ☐ Trash or version-history retention window checked for your primary cloud provider.

#### SCALING TO YOUR TEAM OR ORGANIZATION

For a team, shared drives create shared risk. Designate an owner for your backup process: someone who is responsible for confirming that backups run and that a restore has been tested. A backup no one has tested is a backup you do not actually have. Run a restore test before you need it. For shared drives, apply role-based access from the start: people should have access to the folders their work requires, not everything. When someone leaves the team, removing their access to shared drives should be on the same checklist as disabling their accounts. Unreviewed access accumulates; build the cleanup habit now.

### IF YOU'RE BEING TARGETED

Your most sensitive files should not live in a standard cloud sync folder where they are accessible from any signed-in browser session. Consider keeping your crown jewels in an end-to-end encrypted location: an E2E-encrypted cloud storage service, an encrypted container on a local drive, or a local-first application that does not sync unencrypted copies. An adversary who compromises your cloud account credentials should not immediately have your most sensitive documents. Also consider your backup provider: a backup service that requires only a password to access is as weak as whatever protects that password. Use your password manager and MFA for backup accounts too.

### ▲ COMMON MISTAKES

- Treating cloud sync as a backup. Cloud sync replicates your current state, including deletions and ransomware encryption. A real backup keeps historical versions you can restore from. Confirm your solution keeps versioned copies, not just the current state.
- Backing up to a second folder on the same drive. This protects against accidental deletion but not against drive failure, theft, or ransomware. Off-site means physically separate.
- Never testing a restore. A backup you have never successfully restored from is an assumption, not a backup. Restore a file from backup now, before you need to restore everything.
- Leaving shared links open indefinitely. "Anyone with the link" access does not expire. Documents shared for a one-time purpose years ago may still be publicly accessible. Audit and revoke.
- Forgetting about mobile backups. Your phone likely holds contacts, photos, messages, and authenticator app data. Confirm it backs up automatically, and know what is and is not included in the backup.

**You're done with this pillar when:** your crown jewels are identified, covered by an automatic backup that runs without manual steps, stored in at least three copies with one off-site, your cloud sharing has been audited with "anyone with the link" grants revoked, and you have confirmed encryption is enabled on your cloud storage.

## PILLAR 5 · NETWORK &amp; ENVIRONMENT

# Network & Environment

---

## Why this matters now

Your router is the single chokepoint for every device in your home or office. A compromised router can intercept, redirect, or inspect traffic before any app-level protection can act. Most routers ship with default credentials that are publicly documented and never enforced to change. Phase One does not ask you to become a network engineer. It asks you to close the obvious gaps: replace the defaults, keep firmware current, isolate untrusted devices from your sensitive ones, and use end-to-end encrypted messaging for conversations that need to stay private.

## Do this

Work through these steps in order. The first four have the highest impact and take the least time.

1. **Log in to your router admin panel.** The address is usually printed on a label on the router itself, commonly `192.168.1.1` or `192.168.0.1`. Open it in a browser while connected to the network.
2. **Change the admin password.** Replace the factory default with a strong, unique password generated by your password manager. If the router has a separate admin username, change that too. Save both in your password manager.
3. **Check for firmware updates.** Look for a "Firmware," "Software Update," or "Advanced" section in the admin panel. Install any available updates and restart the router. Some routers support automatic firmware updates; enable that option if present.
4. **Set your Wi-Fi security mode to WPA3 or WPA2-AES.** Older modes (WEP, WPA-TKIP, WPA mixed-mode) have known cryptographic weaknesses. If your router offers WPA3, use it. If not, WPA2-AES (sometimes labeled WPA2-Personal with AES) is the correct fallback. Avoid "TKIP" or "Auto" combinations.
5. **Set a strong, unique Wi-Fi passphrase.** Treat this like an account password: generate it with your password manager, aim for at least 16 characters, and store it there. Change it from any default the router shipped with.
6. **Rename your network (SSID).** Remove the router manufacturer or model name from the default SSID. Do not include your name, apartment number, or any identifying information. A generic or neutral name is fine.
7. **Create a separate guest network.** Enable the guest network feature in your router admin panel. Put all visitors on this network. More importantly, put every IoT device on it too: smart TVs, speakers, cameras, thermostats, and anything else that does not need to reach

your computers or phones directly. Guest networks are isolated from the main LAN by default on most consumer routers.

8. **Disable WPS (Wi-Fi Protected Setup).** WPS has well-documented vulnerabilities that allow brute-force PIN attacks. Find the WPS option in your wireless settings and turn it off. You almost certainly do not use it.
  9. **Disable remote management.** Unless you have a specific reason to administer your router from outside your network, turn off any "Remote Access," "WAN Management," or "Remote Admin" options. These expose your admin interface to the open internet.
  10. **Install Signal on your phone and computer.** For any conversation that carries sensitive information: legal strategy, source communications, organizational planning, financial matters. Signal provides end-to-end encryption by default for messages and calls. Share your Signal number or username only with people who need it. Enable the "Note to Self" feature as a secure scratch pad for sensitive notes you send yourself.
- ☐ Router admin password changed and saved in password manager.
  - ☐ Router firmware updated to current version.
  - ☐ Wi-Fi set to WPA3 or WPA2-AES with a strong, unique passphrase.
  - ☐ Network SSID renamed to something non-identifying.
  - ☐ Guest network created and enabled.
  - ☐ IoT and smart-home devices moved to the guest network.
  - ☐ \* WPS disabled.
  - ☐ Remote management disabled.
  - ☐ Signal installed and used for sensitive conversations.

#### SCALING TO YOUR TEAM OR ORGANIZATION

A single consumer router is not adequate for a team. At the organizational level, the guest network principle becomes formal segmentation: separate VLANs for staff devices, IoT, servers, and guest access, each with its own firewall rules. Any device that needs to reach sensitive systems should be on a controlled segment. Require that all staff router setups follow the personal steps above, especially firmware updates and WPA3. For team communications, deploy Signal at the organizational level, establish a policy on which channels are approved for sensitive topics, and ensure that informal platforms (SMS, consumer chat apps) are not used for organizational matters. If you have a shared office or coworking arrangement, assume the local network is untrusted and act accordingly.

### IF YOU'RE BEING TARGETED

If you are under active surveillance or facing a sophisticated adversary, treat your home network with the same skepticism you would a coffee-shop Wi-Fi. Periodically review the list of connected devices in your router admin panel and investigate anything unfamiliar. Disable UPnP in your router settings. UPnP allows devices and software to open ports on your behalf without your knowledge, which is a persistent source of silent exposure. Consider periodically rotating your Wi-Fi passphrase and re-connecting your devices intentionally. For the most sensitive communications, do not rely on network-level controls: use Signal and assume the path can be observed.

### ▲ COMMON MISTAKES

- Leaving the router on its factory admin password indefinitely. Default credentials for every major consumer router are published online and are the first thing automated scanners try.
- Mixing trusted devices with IoT on the same network. A compromised smart speaker or cheap camera has direct access to your laptop on a flat network.
- Using WPA2 in "mixed mode" or leaving TKIP enabled. Many routers default to a compatibility mode that allows weaker encryption. Set it explicitly to AES-only.
- Assuming a VPN makes router hardening unnecessary. A VPN encrypts traffic in transit but does nothing to protect you from a compromised router on your local network, and nothing to isolate a compromised IoT device from your computers.
- Installing Signal but using it only for casual conversations and reverting to SMS for anything sensitive out of convenience. Signal is only useful if you actually use it for the things that matter.

**You're done with this pillar when:** your router has a changed admin password, current firmware, WPA3 or WPA2-AES, a separate guest network carrying all IoT and visitor devices, WPS off, remote management off, and Signal is installed and in active use for sensitive conversations.

## PILLAR 6 · AUTOMATION &amp; ORCHESTRATION

# Automation: Make Security Automatic

---

## Why this matters now

Friction is the enemy of consistent security. When doing the right thing requires extra steps, remembering a schedule, or interrupting what you are working on, it will slip. Updates get deferred for a week, then a month. Backups run manually until they stop running at all. Passwords get reused because the generator was not active at the moment of account creation. Phase One automation is not complicated: it means flipping the switches that make good decisions happen without your involvement, and adding one recurring appointment to your calendar so nothing drifts permanently. Do this once and the maintenance cost drops to near zero.

## Do this

### 1. Enable automatic OS updates on every device you own.

- On macOS: System Settings > General > Software Update > enable "Automatic Updates," including "Install Security Responses and System Files."
- On Windows: Settings > Windows Update > enable "Receive updates for other Microsoft products" and confirm Active Hours are set so restarts do not interrupt work at a bad time.
- On iOS: Settings > General > Software Update > Automatic Updates > enable both download and install.
- On Android: Settings > System > System Update > enable automatic updates. Also check your manufacturer's security update setting if it exists separately.

### 2. Enable automatic app updates on every device.

- On macOS: App Store > Preferences > enable "Automatic Updates."
- On iOS: Settings > App Store > enable "App Updates."
- On Android: Google Play > Settings > Network Preferences > Auto-update apps > set to "Over any network" or "Over Wi-Fi only" depending on your data situation.
- For apps installed outside the App Store or Play Store: identify how each updates (built-in updater, package manager, manual download) and set them to automatic where possible.

### 3. Enable automatic browser updates.

Most modern browsers update automatically when you restart them, but verify this. In Chrome, go to the menu and check for updates. In Firefox, go to Settings > General > Firefox Updates > "Install updates automatically." In Safari, updates come through macOS system updates. Make a habit of restarting your browser when you see an update badge rather than dismissing it.



4. **Turn on password manager autofill.** Open your password manager settings and confirm the browser extension or system integration is active on every device and browser you use. Autofill does two things: it stops you from manually retyping passwords (which invites re-use) and it defeats most phishing by refusing to fill credentials on a domain that does not match the saved entry.
5. **Confirm password generation is configured to strong defaults.** In your password manager settings, set generated passwords to at least 16 characters, using letters, numbers, and symbols. Set this as the default so every new account gets a strong password without extra effort at the moment of creation.
6. **Verify your automatic backup is running.** Go back to your Pillar 4 backup setup and confirm the scheduled job is active and has completed at least one successful backup. Do not assume it is working: look at the last-run timestamp in the backup software. If it has not run since you configured it, investigate and fix the schedule now. Set the backup interval to daily if your data changes frequently, or weekly at minimum.
7. **Enable automatic screen lock on every device.** Set the inactivity timeout to five minutes or less. This is not glamorous, but an unlocked device left on a desk for ten minutes undoes most of the security you have built.
8. **Schedule a recurring quarterly security review.** Open your calendar and create a repeating event every three months titled "Quarterly Security Review." Set it to a time when you are not rushed. In the event notes, include a short checklist: review accounts in your password manager for any still using weak or reused passwords, confirm backups are running and recent, check for any unrecognized devices on key accounts, and review which apps have permissions they no longer need. A quarterly review prevents the slow drift where individual decisions accumulate into a weak posture over time.

- ☐ Automatic OS updates enabled on all devices.
- ☐ Automatic app updates enabled on all devices.
- ☐ Browser set to install updates automatically.
- ☐ Password manager autofill active in every browser and on every device.
- ☐ Password generator defaults set to 16+ characters with symbols.
- ☐ Automatic backup confirmed running with a recent successful completion.
- ☐ Screen lock inactivity timeout set to five minutes or less on all devices.
- ☐ Quarterly security review on the calendar as a recurring event.



### SCALING TO YOUR TEAM OR ORGANIZATION

Manual enforcement of update policies across a team does not hold. Use mobile device management (MDM) to enforce OS and app update compliance and to report devices that are falling behind. Most MDM tools let you set a maximum number of days a device can defer a security update before it loses access to organizational resources. For backups, move from individual responsibility to centralized monitoring: whoever manages infrastructure should be able to confirm that all enrolled devices are backing up on schedule. The quarterly review becomes a formal process: a designated person runs it, documents findings, and closes any gaps before the next cycle. The goal is the same as the personal version, removing the dependency on anyone remembering to do it.

### IF YOU'RE BEING TARGETED

For high-risk individuals, zero-day and n-day exploits targeting unpatched software are a real attack vector, not a theoretical one. Install security updates within 24 hours on your primary devices, not the default seven-day window. Do not defer restarts. For your most sensitive device, consider shortening the backup interval to hourly if your backup software supports it, so a ransomware event or device seizure does not cost you more than an hour of work. The quarterly review should also include a brief check for signs of compromise: look at your process list for unfamiliar names, review recent logins in your key accounts, and check whether any new browser extensions appeared that you did not install.

### ▲ COMMON MISTAKES

- Enabling automatic updates but never restarting devices. Updates that are downloaded but not installed are not applied. Many OS updates require a restart to take effect. An update pending for three weeks provides no protection.
- Configuring automatic backups without checking that they ran. Backup software fails silently: a full disk, a disconnected drive, a changed account password, or a misconfiguration can stop backups while the scheduler still shows "active." Look at the last-completed timestamp.
- Setting a password generator to the minimum allowed length rather than a strong default. Many sites accept 8-character passwords. Your generator should not be set to 8 just because it is permitted.
- Treating the quarterly review as optional and skipping it when busy. This is the one manual step that does not automate. If you skip it, the slow drift that automation prevents in the short term accumulates over months until something significant is out of date.

**You're done with this pillar when:** automatic updates are on for your OS, apps, and browser on every device; your password manager is set to autofill and generate strong passwords by default; your backup is confirmed running on schedule; your screen locks within five minutes; and a quarterly security review is on your calendar as a recurring event.

## PILLAR 7 · VISIBILITY &amp; ANALYTICS

# Visibility & Awareness

---

## Why this matters now

You cannot defend what you cannot see. Most people learn they have been compromised from an external source: a friend's warning, a breach notification email, a credit alert, weeks or months after the fact. By then the damage is done and the attacker has had time to pivot. Phase One visibility is about closing that gap. You establish a baseline by checking what has already been exposed, you turn on alerting so future events surface quickly, and you learn to recognize phishing before you click. None of this requires special tools. It requires looking at the right places once, then keeping alerts active so you do not have to keep looking.

## Do this

1. **Check every email address you use on Have I Been Pwned.** Go to [haveibeenpwned.com](https://haveibeenpwned.com) (<https://haveibeenpwned.com>) and enter each email address you own, including old addresses you still use for logins. The site shows which known data breaches included your address and what categories of data were exposed (passwords, phone numbers, physical addresses, and so on).
2. **Act on every breach that exposed a password.** For any service that shows a password breach, go to that service and change the password now, using your password manager to generate a new unique one. If you reused that password anywhere else, change it there too. If the service supports MFA and you have not enabled it, do that at the same time.
3. **Enable login and sign-in alerts on your email accounts.** Your email account is your identity anchor: access to it unlocks password resets for nearly everything else. Turn on security alerts for new sign-ins.
  - Gmail: Security > Recent security activity > confirm alerts are active. Google sends automatic alerts for new device sign-ins; verify your recovery email and phone are current.
  - Outlook or Microsoft account: Security > Advanced security options > enable "Get alerts and action recommendations."
  - Other providers: look for "Security alerts," "Login notifications," or "Sign-in activity" in account security settings.
4. **Enable sign-in alerts on financial accounts.** Log in to each bank, credit union, brokerage, and payment service you use. Find the notification settings and turn on alerts for any new login, password change, or new device. Many financial institutions send these by email and SMS. Enable both.

**5. Review which devices and sessions are currently signed in to your key accounts.** Do this for your primary email, your Apple ID or Google account, and any other account that has broad access to your data.

- Google: [myaccount.google.com/device-activity](https://myaccount.google.com/device-activity) (<https://myaccount.google.com/device-activity>)
- Apple ID: Settings (on iPhone) or System Settings (on Mac) > your name > scroll down to see signed-in devices.
- Microsoft: [account.microsoft.com/devices](https://account.microsoft.com/devices) (<https://account.microsoft.com/devices>)

Remove any device or session you do not recognize. If you find something unexpected, treat it as a compromise: change the account password immediately, review recent activity, and check whether any forwarding rules or authorized apps were added without your knowledge.

**6. Sign up for breach monitoring.** Have I Been Pwned offers a free notification service. Enter your email addresses and choose to be notified when they appear in future breaches. This means you learn about new exposures when they happen rather than when you happen to check.

**7. Learn the phishing red flags.** Phishing is the most common initial access method across all threat levels. Recognizing it is a skill, not intuition. The consistent markers are:

- Urgency or threat: "Your account will be closed in 24 hours," "Immediate action required."
- A sender address that does not match the organization it claims to be from. Look at the actual domain after the @ symbol, not just the display name.
- A link whose destination does not match the claimed site. Hover over links before clicking. On mobile, press and hold to see the full URL.
- A request for credentials, payment information, or MFA codes. Legitimate services do not ask you to enter your password through an emailed link.
- An unexpected attachment, especially one asking you to enable macros or ignore a security warning.
- A message that creates a plausible but unexpected scenario: a package you did not order, an invoice for a service you do not use, a document shared by a colleague you need to verify.

When in doubt about a message, do not click the link in the message. Go directly to the service by typing its address or using your saved bookmark.

- ☐ All email addresses checked on Have I Been Pwned.
- ☐ Passwords changed for every breached service that exposed a password.
- ☐ Sign-in alerts active on all email accounts.
- ☐ Sign-in alerts active on all financial accounts.
- ☐ Signed-in devices and active sessions reviewed on Google, Apple, and Microsoft accounts.

- ☐ \* Unrecognized sessions removed.
- ☐ Have I Been Pwned breach notification email confirmed.
- ☐ Phishing red flags reviewed and understood.

### SCALING TO YOUR TEAM OR ORGANIZATION

At the organizational level, visibility means knowing what is happening across accounts and devices, not just your own. Enable audit logging in your email and collaboration platform (G Suite audit logs, Microsoft 365 Unified Audit Log) and designate someone to check for anomalous activity: logins from unexpected countries, bulk download of files, new mail forwarding rules, or OAuth app grants. Run Have I Been Pwned's domain monitoring on your organization's domain so you are notified when any address on your domain appears in a breach. Brief your team on phishing red flags at least annually. The single most effective way to reduce phishing risk in a team is making it easy and expected for people to forward suspicious messages to whoever handles security, without fear of embarrassment for nearly clicking something.

### IF YOU'RE BEING TARGETED

Sophisticated phishing directed at you personally will be harder to spot than generic lures. Adversaries do reconnaissance first: they know who you work with, what projects you are on, and what requests would seem plausible from a trusted contact. If you are in a high-risk category, treat any unexpected request that involves credentials, a link, an attachment, or a payment with heightened skepticism, even if it appears to come from someone you know. Verify through a separate channel (call the person, use a different messaging thread) before acting. Also check your active email rules and forwarding settings periodically: a common persistence technique after account compromise is to add a silent forwarding rule that copies your email to an attacker-controlled address. This rule survives a password change if you do not find and remove it.

### ▲ COMMON MISTAKES

- Checking Have I Been Pwned once and never returning. New breaches are added continuously. The free notification service is the right replacement for manual spot-checks.
- Seeing a breach result and doing nothing because the breach is old. Old password breaches still matter if the password was reused anywhere that is still active.
- Dismissing login alerts without reading them. An alert for a new device sign-in from an unexpected city or browser is worth investigating, not archiving.
- Leaving unrecognized sessions in place. If you see a device or session you do not recognize and cannot account for, assume the worst and remove it. An explanation you cannot verify is not reassurance.
- Trusting the sender display name on an email. Display names are trivially spoofed. The actual sending address is what matters, and even that can be spoofed in some configurations. The content and the request are the real signal.

**You're done with this pillar when:** every email address has been checked on Have I Been Pwned and breach notifications are active, sign-in alerts are on for your email and financial accounts, you have reviewed and cleaned up signed-in devices on your key accounts, and you can identify the main phishing red flags without a checklist in front of you.

# Phase One Completion Checklist

---

Use this checklist after working through all seven pillar chapters, not as a substitute for reading them. Each item maps to concrete steps covered in the relevant chapter. Every box must be checked before you move to Phase Two.

## Pillar 1: User

- ☐ A password manager is installed and set up on all your primary devices.
- ☐ Your email, banking, and other top accounts each have a unique, generated password stored in the manager.
- ☐ All remaining accounts have been updated to unique passwords in the manager.
- ☐ MFA is enabled on your email, financial, and primary identity accounts.
- ☐ Recovery codes for every MFA-protected account are stored offline in a secure location.
- ☐ Account recovery on your email provider is locked down: SMS recovery removed or secured.
- ☐ Your phone number is protected against SIM-swap and unauthorized porting.

## Pillar 2: Device

- ☐ Automatic OS updates are enabled on every device you own.
- ☐ Device encryption is verified and active on every computer and mobile device.
- ☐ Every device has a strong lock code or passphrase set.
- ☐ Find My or equivalent remote-wipe capability is enabled on every mobile device.
- ☐ You have a simple inventory of every device that touches your accounts or data.

## Pillar 3: Apps & Software

- ☐ You have a full list of installed apps and have uninstalled everything you do not actively use.
- ☐ Permissions (location, microphone, camera, contacts) have been reviewed and trimmed on your most-used apps.
- ☐ Automatic updates are enabled for all remaining apps.
- ☐ You have chosen one well-maintained browser as your primary and removed or disabled others.
- ☐ Your primary browser has basic hardening applied: third-party cookies blocked, HTTPS-only mode on.

## Pillar 4: Data

- ☐ You have identified your crown jewels: the data, files, and accounts most critical to protect or most damaging if lost.
- ☐ Automatic backups run to at least two destinations (local and cloud).
- ☐ You have confirmed the backup actually ran and contains your most important files.

- ☐ Encryption is enabled on your primary cloud storage account.
- ☐ Publicly shared or over-shared links and folders have been audited and cleaned up.

## **Pillar 5: Network & Environment**

- ☐ Your router admin password is changed from the factory default.
- ☐ Router firmware is updated to the current available release.
- ☐ Your Wi-Fi network uses WPA3 or WPA2-AES with a strong, unique passphrase.
- ☐ A separate guest or IoT network is set up and in use for visitors and smart-home devices.
- ☐ Signal is installed and configured for sensitive conversations.

## **Pillar 6: Automation**

- ☐ Automatic OS and firmware updates are confirmed enabled on every device (cross-check with Pillar 2).
- ☐ Backups are scheduled to run automatically without manual action.
- ☐ Password-manager autofill and automatic password generation are active in your browser.
- ☐ A recurring quarterly security review reminder is on your calendar.

## **Pillar 7: Visibility & Awareness**

- ☐ You have checked all your email addresses on Have I Been Pwned and acted on any confirmed breaches.
- ☐ Login alerts and sign-in notifications are enabled on your email and financial accounts.
- ☐ You have reviewed active devices and sessions on each key account and removed any you do not recognize.
- ☐ You can identify the core phishing red flags: spoofed senders, urgency pressure, unexpected attachments, mismatched links.

## Appendix A: NSA Phase One Crosswalk

This guide follows the same seven-pillar structure as the NSA Zero Trust Implementation Guideline. The table below maps each chapter in this guide to its corresponding NSA pillar and lists representative NSA Phase One capabilities from that pillar. NSA Phase One defines 36 Activities and 30 Capabilities aimed at establishing a secure foundation. This crosswalk is representative, not exhaustive: the NSA document contains additional capabilities and sub-activities not listed here.

The NSA ZIG is a U.S. government public-domain work. This guide is an independent civilian adaptation; see the About section for the full disclaimer.

*Crosswalk: This Guide to NSA Zero Trust Implementation Guideline Phase One*

This guide's pillar	NSA pillar	Representative NSA Phase One capabilities
User	User	Multi-Factor Authentication; Privileged Access Management; Identity Lifecycle Management; Least Privileged Access
Device	Device	Device Health Verification; Comply-to-Connect foundations; Device Inventory
Apps & Software	Application & Workload	Application Inventory; Authorized Application Use; Application Permission Governance
Data	Data	Data Tagging Foundations; Data Classification; Encryption at Rest
Network & Environment	Network & Environment	Network Segmentation Foundations; Encrypted Wireless; Traffic Filtering Basics
Automation	Automation & Orchestration	Automated Patch Management; Backup Automation; Password Management Automation
Visibility & Awareness	Visibility & Analytics	Log Collection Foundations; Sign-in Alerting; Breach Exposure Monitoring

### NOTE

Phase Two of this series maps to NSA Phase Two, which adds 41 Activities and 34 Capabilities focused on integrating distinct Zero Trust solutions, including EDR/XDR, micro-segmentation, DLP/DRM, SOAR, and analytics at scale.



## Appendix B: Sources & Acknowledgements

---

The following sources informed this guide. Where a source is a U.S. government publication, it is in the public domain. This guide is an independent civilian adaptation; Houston Labs LLC is not affiliated with, authorized by, or endorsed by any of the government agencies listed below.

### Primary Sources

#### NSA Zero Trust Implementation Guideline: Phase One (January 2026)

The primary source this guide adapts. Published by the National Security Agency. Defines 36 Activities and 30 Capabilities for establishing a secure Zero Trust foundation across seven pillars. U.S. government public-domain work. Available from the NSA Cybersecurity Directorate.

#### Houston Labs Civilian Zero Trust Primer (2026)

The conceptual companion to this guide. Establishes the threat model, introduces the seven-pillar framework, and explains why Zero Trust applies to civilians. Read the Primer before this guide. Published by Houston Labs LLC.

#### NSA Cybersecurity Information Sheet: Embracing a Zero Trust Security Model (2021)

An earlier NSA document defining Zero Trust principles and the seven-pillar model at a conceptual level. U.S. government public-domain work. Available from the NSA Cybersecurity Directorate.

### Supporting Standards

#### NIST Special Publication 800-207: Zero Trust Architecture (2020)

The foundational U.S. federal standard for Zero Trust architecture. Defines tenets, logical components, and deployment models. U.S. government public-domain work. Published by the National Institute of Standards and Technology.

#### CISA Zero Trust Maturity Model, Version 2.0 (2023)

A maturity model for federal agencies, also widely used as a civilian reference. Defines five maturity stages across five pillars. U.S. government public-domain work. Published by the Cybersecurity and Infrastructure Security Agency.

### Public-Domain Note

Works produced by U.S. government employees as part of their official duties are in the public domain within the United States and are not subject to copyright protection under 17 U.S.C. § 105. The NSA and NIST publications listed above fall into this category. Houston Labs LLC's original expression in this guide, including all civilian framing, editorial organization, and added content, is the independent intellectual work of Houston Labs LLC and is not a U.S. government work.

## **Independent Publication Disclaimer**

This guide is published independently by Houston Labs LLC. It is not affiliated with, authorized by, sponsored by, or endorsed by the National Security Agency, the National Institute of Standards and Technology, the Cybersecurity and Infrastructure Security Agency, or any other agency or department of the U.S. government. Reference to those organizations and their publications is for attribution and informational purposes only.