SECURITY POLICY

How To Write A One-Page Cybersecurity Policy

Plain-English how-to. ~90 minutes. Includes a fill-in template you can use today.

If asked, most small business owners say 'we have security practices but no formal policy.' That's a problem. Without a written, signed policy: employees aren't accountable, cyber insurance is harder to get, customer contracts may fall through, and breach response is improvised.

But cybersecurity policies don't have to be 50 pages of legalese. A one-page document covering the critical practices, with everyone's signature on the back, gets you 80% of the benefit at 5% of the effort.

By the end of this guide you'll have a one-page cybersecurity policy customized for your business, signed by every employee, posted in a visible place, and integrated with onboarding. You'll have done in 90 minutes what most businesses never get around to.

Quick snapshot

What you'll learn	Write, sign, and operationalize a one-page cyber policy for your business.
Skill level	Owner / HR / IT lead
Time required	90 minutes
What you'll need	This template, your current practices, leadership buy-in
Risk if you skip this	No accountability, harder insurance, weaker contracts, improvised incident response
PDF kit	■ Download at the bottom of this page

Why this matters

Written policy turns 'we should do this' into 'this is required.' It's the difference between intent and accountability. Insurance carriers, auditors, and large customers all ask for it.

Many large customers now include cybersecurity clauses in vendor contracts. A written policy lets you answer 'yes' confidently — and not lose a deal because of a checkbox question.

When an incident happens, having a documented baseline of practices matters legally. 'We had a policy and an employee violated it' is a defensible position; 'we never wrote it down' is not.

Before you start

Inventory what you actually do today — MFA, password practices, training, backups, incident response. Policy should document reality, not aspirational goals.

Get leadership commitment to enforcing the policy. An unsigned, unenforced policy is worse than none — it shows bad faith.

Have your attorney review the final draft. Especially for any references to data handling, regulated information, or termination consequences.

Step 1 — Use this template structure (one page, 7 sections)

1. Purpose (2 sentences). **2. Scope** (1 sentence — who and what). **3. Account & Authentication**. **4. Device & Network**. **5. Data Handling**. **6. Incident Reporting**. **7. Acknowledgment** (signature line).

Each section is 2-4 sentences. The whole document fits on one printed page. Resist the urge to expand — single-page policies actually get read.

Step 2 — Section 3: Account & Authentication

Sample text: *'All employee accounts must use multi-factor authentication. Passwords must be at least 14 characters, unique per service, and stored in the company-approved password manager. Employees may not share credentials with anyone, including coworkers or family members.'*

Three concrete rules. Specific. Enforceable. No ambiguity.

Step 3 — Section 4: Device & Network

Sample text: *'Company-owned devices must have automatic updates enabled, full-disk encryption on, and require a password to unlock. Personal devices used for work must enroll in our MDM (Mobile Device Management) before accessing email. Public WiFi requires VPN.'*

Tailor to what you actually require. If you don't have MDM, remove the line — don't pretend.

Step 4 — Section 5: Data Handling

Sample text: *'Customer data may not be stored on local laptops or personal cloud accounts. All customer data lives in [approved system]. Sharing customer data with third parties requires written approval from the owner.'*

Get specific about your approved systems (Salesforce, QuickBooks Online, your CRM). If you have regulated data (HIPAA, PCI), add a sentence.

Step 5 — Section 6: Incident Reporting

Sample text: *'Employees must report suspected security incidents — phishing, lost devices, suspicious activity — immediately to [contact] via [channel]. There is no penalty for reporting in good faith. Failing to report a known incident is grounds for disciplinary action.'*

The no-blame, must-report combination is critical. Reward reporting; punish hiding.

Step 6 — Section 7: Acknowledgment

Sample text: *'I have read and understand the [Company Name] Cybersecurity Policy. I agree to follow these practices in my work. Signature: _____ Date: _____'*

Every employee signs. New hires sign on day 1. Update the policy and re-sign annually.

Step 7 — Roll it out

20-minute all-hands meeting. Walk through the policy. Each section: 1-minute summary + Q&A.; Have everyone sign at the end. Done.

Post a printed copy in a common area or pinned in your team chat. Visibility matters for sustained compliance.

Step 8 — Maintain and update annually

Calendar a yearly policy review. 30 minutes: 'What changed in our practices this year? What new threats emerged? What sentences need updating?'

After any incident or major change (new SaaS, new building, new regulation), update the policy too. Outdated policies undermine the culture they're supposed to build.

PRO TIP

Real Beats Aspirational.

Document what you actually do, not what you wish you did.

Single-page policies get read. Multi-page ones don't.

Concrete rules (MFA required) beat vague ones (use 'strong authentication').

Update annually. Outdated policy = no policy.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Add appendices for regulated data

Keep the main policy one page, but add an appendix per regulation (HIPAA, PCI, GDPR) as needed.

Trade-off: more pages; reserve for required compliance.

Power-user upgrade #2 — Align to a published framework

CIS Controls v8 IG1 or NIST CSF maps your policy to industry baselines. Useful for insurance and audits.

Trade-off: extra documentation.

Power-user upgrade #3 — Use a policy management platform

Vanta, Drata, Tugboat Logic — automate distribution, signature collection, training records.

Trade-off: subscription cost.

Power-user upgrade #4 — Add a vendor/third-party management section

If you handle data through vendors, add expected security practices and DPA requirements.

Trade-off: more legal review.

Power-user upgrade #5 — Tie to performance reviews

Include 'follows cybersecurity policy' as a review criterion. Reinforces it as a baseline expectation.

Trade-off: requires HR coordination.

Power-user upgrade #6 — Add an AI usage section

Cover what AI tools employees can use (and what data they may not paste). This is the fastest-evolving policy area in 2025-2026.

Trade-off: requires periodic updates.

Common mistakes & pitfalls

Mistake — Writing 50-page policies nobody reads.

Fix — One page beats fifty. Concise is enforceable.

Mistake — Documenting aspirations as policy.

Fix — Policy must reflect reality. Aspirations belong in a roadmap.

Mistake — Skipping the signature.

Fix — Without signed acknowledgment, accountability is unclear.

Mistake — Never updating the policy.

Fix — Outdated policy is worse than none. Annual review minimum.

Mistake — No incident reporting clause.

Fix — Without one, breaches go unreported until catastrophic.

Mistake — Mixing aspirational and binding language.

Fix — Use 'must' for required; use 'should' sparingly and only for genuine guidance.

Mistake — No leadership signature.

Fix — Owner / CEO signs first. Modeling matters.

Pro tips

Pro tip 1. Use plain English. If your attorney rewrites it in legalese, push back.

Pro tip 2. Post a poster-size version in the office break room.

Pro tip 3. Reference the policy when training: 'This is why we have rule #3.'

Pro tip 4. Track signatures in HR system. Easy audit trail for insurance.

Pro tip 5. Share the policy publicly (your security page) if possible — signals maturity to customers.

Frequently asked questions

Do I need an attorney to write this?

You can draft it yourself using this template. Have an attorney review the final draft, especially termination/discipline language and regulated-data sections.

How does this affect cyber insurance pricing?

Documented, signed policies typically reduce premiums and broaden coverage options. Many carriers require it.

What if employees won't sign?

Have a clear leadership message. Resistance usually means the policy contradicts current practice — fix one or the other. If individuals still refuse, treat it as the HR issue it is.

Do I need separate policies for full-time, part-time, and contractors?

The same policy can cover all three. Contractors should sign as part of their MSA. Part-time and full-time sign during onboarding.

How often should I update?

Annually minimum. After any incident or major operational change. After new regulations (e.g., new state privacy laws).

Should I publish my policy publicly?

Many companies publish a security page summarizing their practices (without the internal disciplinary language). It signals maturity to customers.

What about AI tools — should I add a policy now?

Yes — by 2026, AI usage policy is one of the most-asked-about sections. Cover: which tools approved, what data may not be shared, how to verify AI output.

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

1. Use the 7-section one-page template.
2. Document reality, not aspiration.
3. Use 'must' for required, 'should' rarely.
4. Include a no-blame incident reporting clause.
5. Have every employee sign — leadership first.
6. Post and reference visibly.
7. Review annually; update after incidents.
8. Add an AI usage section by 2026.

Mini glossary

AUP: Acceptable Use Policy — defines what employees may do with company systems.

DPA: Data Processing Agreement — vendor contract addendum about data handling.

CIS Controls: Industry-standard baseline of cybersecurity controls.

NIST CSF: NIST Cybersecurity Framework — government-published model.

MDM: Mobile Device Management — central control of phones/tablets.

Acknowledgment: Employee's signed statement of understanding and agreement.