QUICK REFERENCE

Security Policy Templates Quick Reference

Seven non-negotiable rules every small business should publish — and the discipline framework to enforce them fairly.

Non-Negotiable Rules for Every Employee

1. Use Strong, Unique Passwords

- At least 12 characters
- Never reuse passwords across sites
- Use the company password manager (Bitwarden, 1Password, etc.)
- Never share passwords — not even with coworkers you trust

2. Enable Multi-Factor Authentication (MFA)

- **Email** — required (criminals use email to reset every other password)
- **Banking** — required
- **Any system holding customer data** — required
- **Business social media accounts** — required

3. Lock Your Computer When You Walk Away

Always, even for one minute. Set auto-lock to 5 minutes as a safety net.

4. Think Before You Click

- Do not click suspicious links
- Do not open unexpected attachments
- Verify before acting on urgent requests — call the sender on a known number
- When in doubt, ask before you click

5. Report Security Problems Immediately

If you clicked something suspicious, lost a device, sent data to the wrong person, or anything feels wrong — report it right away. Early reports are rewarded. Hidden mistakes are what become disasters.

6. Protect Customer Information

- Never email unencrypted customer data
- Do not leave records where others can see them
- Shred physical documents when done
- Only access what you need for your job

7. Follow Company Policies

On acceptable use of computers, social media, data handling, and vendor access.

Password Policy Template

- ✓ Minimum 12 characters — longer is better
- ✓ Mix of letters, numbers, and symbols
- ✓ No dictionary words, names, or dates tied to you
- ✓ Different password for every account

- ✓ Stored in the company-approved password manager (not in browsers, not in documents)
- ✓ Rotated immediately if compromised (no arbitrary 90-day rotation — it backfires)

Acceptable Use Policy (Core Clauses)

- **Company equipment** is for business use. Limited personal use is allowed but should not interfere with work.
- **No personal confidential data** — employees should not store their own financial or medical data on company systems.
- **No unauthorized software** — installs require approval from [designated person].
- **No unauthorized AI tools** with customer or financial data (see the AI Acceptable-Use Quick Reference).
- **Monitoring notice** — company may review activity on company systems as part of operations and security.

Progressive Discipline Framework

Philosophy: Security culture depends on people feeling safe to report mistakes. Punishing honest errors guarantees the next one will be hidden. Reserve discipline for *intentional* violations, repeated errors after training, or hiding incidents.

- ✓ **First unintentional violation:** Conversation, additional training, documented
- ✓ **Second unintentional violation:** Written warning, mandatory retraining
- ✓ **Third unintentional violation:** Formal performance improvement plan
- ✓ **Intentional violations / hiding incidents / theft:** Immediate formal discipline up to termination

Culture Beats Policy

The best policy is one employees actually understand and follow. Short, plain-language policies signed at onboarding and reinforced quarterly will outperform a 40-page document nobody reads. Make the reporting line obvious (one email address, one phone number) and thank people when they use it.