

Password Policy Template

Template · A Plain-Language Password Policy For Families Or Small Businesses.

Adopt this as-is or edit to match your context. Customise the brackets, adopt the rules, have everyone sign. Review annually.

Scope

This password policy applies to all members of [household name / business name] and any device, account, or service used for [household / business] purposes.

Effective date: _____ · Owner: _____

Required Practices

- 1 **Use a password manager.** [Manager name, e.g., 1Password, Bitwarden] is the approved tool. Master password must be 16+ characters and never reused.
- 2 **Unique passwords per account.** No reuse, ever. The password manager generates and stores them.
- 3 **Minimum length: 16 characters.** Generated by the password manager.
- 4 **Multi-Factor Authentication (MFA) required** on email, banking, brokerage, password manager, cloud storage, and any work-related account.
- 5 **MFA via authenticator app preferred.** SMS-based MFA only when no other option exists.
- 6 **Recovery codes saved** in the password manager's Secure Notes section AND printed and stored in [physical location, e.g., fire safe].
- 7 **No sharing of passwords via email, text, or chat.** Use the password manager's secure-share feature.

Prohibited Practices

- Reusing passwords across accounts.
- Storing passwords in plaintext (sticky notes, .txt files, browser-only without manager).
- Sharing personal master password with anyone.
- Using SMS-only MFA on critical accounts when authenticator app is available.
- Disabling MFA after it has been set up.

Rotation Triggers

Passwords must be changed when any of the following occur:

- The service experiences a public data breach.
- Have I Been Pwned alert shows the password is compromised.
- An employee leaves the business / household member changes status.
- Suspicion of unauthorised access (login alerts from unknown locations, etc.).

Otherwise: no scheduled rotation required (modern guidance no longer recommends arbitrary periodic changes for users with strong unique passwords + MFA).

Acknowledgement

I have read this policy and agree to follow it. I understand that violating this policy exposes the [household / business] to security risks.

Name: _____ Date: _____

Signature: _____

Annual Review

Last reviewed: _____ · Reviewer: _____ · Next review: _____

READ NEXT

Why SMS-Based MFA Is Worse Than No MFA At All.

SIM-swap attacks bypass text-message 2FA in minutes. Here's what to use instead — and how to migrate every account in under 30 minutes.

[Visit Making Sense Of Security →](#)