

Password and multi-factor authentication policy

A short, usable policy you can adapt and hand to staff. Written to be read, not filed.

Free to use and adapt. Replace **[Company]** throughout.

Purpose

This policy sets out how everyone at **[Company]** signs in to company systems. It exists to protect client information and to keep the business insurable.

It applies to everyone: staff, contractors, and anyone else with an account.

Before you adopt this. Parts of this policy touch employment terms. Check it against your employment agreements and staff handbook, and take advice if you are unsure. Disciplinary consequences are deliberately left out, because they belong in your HR policy rather than your IT one.

1. Every person gets their own account

- Accounts are personal. **Do not share logins**, including with colleagues you trust.
- If several people need access to the same thing, ask for shared access to be set up properly

rather than passing a password around.

- You are responsible for what happens under your account.

2. Multi-factor authentication is mandatory

- Multi-factor authentication is required on every account that supports it, without exception.
- Use an authenticator app where possible. It is more secure than text messages.
- **Never approve a sign-in prompt you did not trigger.** If one appears unexpectedly, deny it

and report it immediately. That prompt means someone has your password.

3. Passwords

- Use the company password manager for every work account.
- Let the password manager generate passwords. Do not invent them.
- Never reuse a work password anywhere else, especially not on personal accounts.
- Minimum length **[14]** characters where you must set one yourself.
- Passwords are not rotated on a schedule. Modern guidance is that forced rotation makes

passwords weaker, not stronger. Change a password when there is a reason to.

- Passwords are checked against known-breached lists. Every major password manager and Microsoft

Entra ID does this at no extra cost, and it catches the real failure: a password that was fine until it turned up in somebody else's breach.

4. Change a password immediately if

- You receive an unexpected multi-factor prompt
- You entered it on a site that turned out to be fake
- You typed it somewhere unusual and are not sure why you were asked
- A device holding it is lost or stolen
- Anyone else has learned it, for any reason

Report all of the above as well as changing it. Reporting is not getting in trouble. Not reporting is how a small problem becomes a large one.

5. Devices

- Lock your screen when you step away
- Do not save work passwords in a browser. Use the password manager.
- Report a lost or stolen device the same day, no matter the hour

6. Leaving

Access is removed on your last day. Return all company devices and access cards.

What we ask of the business, not just staff

- ☐ Multi-factor authentication enforced centrally, not left optional
- ☐ A password manager provided and paid for by the company
- ☐ Administrator accounts separate from everyday accounts
- ☐ Access reviewed periodically and removed when no longer needed
- ☐ Same-day removal when someone leaves
- ☐ **One emergency access account**, excluded from conditional access, with a long unique password stored offline in a safe or sealed envelope, and tested twice a year. Without one, a policy mistake locks everybody out of the tenant and the only fix is a support case with Microsoft

A policy that asks staff to be careful while the company leaves multi-factor optional is not a policy. It is a hope.

Policy owner: [name] · **Last reviewed:** [date] · **Next review:** [date]

About this template. Free to use, edit, and share, including commercially. No credit needed and no permission required. It is a starting point built from common practice. It is not legal advice, not a compliance certification, and not a substitute for advice about your situation. Your obligations depend on your industry, your regulator, your insurer, and your contracts. If you are in a regulated field, have someone qualified review this before you rely on it.

Last reviewed: August 2026 · Latest version: brevitytech.ca/templates

Made by **Brevity.Tech**, managed IT and automation for small businesses in Metro Vancouver. We roll out password managers and enforce multi-factor as part of every plan. brevitytech.ca · 778-321-2372