

Acceptable Use Policy, Short Form

A short, readable policy that staff will actually finish. Adapt the bracketed parts and have everyone sign it.

This is a starting draft, not a legal document. Brevity.Tech is not a law firm. This is an employment document that imposes obligations on employees, and employment and privacy law in BC affects how you introduce one, particularly to existing staff. Have an employment lawyer review it before you ask anyone to sign.

[Company name] Acceptable Use Policy

This covers the devices, accounts and data you use for work.

Accounts

Your account is yours alone. Do not share your password with anyone, including colleagues and including management. If somebody needs access to something, ask and it will be arranged properly.

Multi-factor authentication is required on all accounts. If you get a prompt you did not trigger, do not approve it, and tell [named person] immediately.

Use the company password manager for work credentials. Do not keep them in a browser, a document, or on paper.

Devices

Keep devices locked when unattended and encrypted at all times. Install updates when prompted rather than deferring them indefinitely.

If you use a personal device for work, company data stays in the managed area of that device and may be removed remotely when you leave or if the device is lost.

Report a lost or stolen device the same day, however embarrassing the circumstances. Speed matters more than anything else and nobody will be in trouble for reporting quickly.

Email and payments

Treat unexpected attachments and links with suspicion, especially when they create urgency.

Any request to change bank or payment details is verified by phone, on a number we already had, before anything moves. This applies regardless of who appears to have sent it.

Nobody will ever be criticized for pausing a payment to check.

Data

Only access what you need for your role. Do not move company data to personal accounts, personal cloud storage, or personal email.

Before pasting company or client information into any external tool, including AI assistants, check with [named person] which tools are approved and on what account.

Personal use

Reasonable personal use of company devices and internet is [permitted / not permitted]. Keep personal files in a personal account rather than company storage, so nothing of yours is caught up if a device is wiped or an account is closed.

Monitoring

[Choose one and be accurate. Silence is not neutral here, and under BC PIPA employee personal information may generally only be collected with notice.]

If you do not monitor: We do not routinely monitor individual email, browsing or file activity. Systems keep security and access logs, and those may be reviewed if there is a specific concern, a suspected security incident, or a legal obligation.

If you do monitor: We monitor [state exactly what, for example email filtering, endpoint security alerts, web filtering]. It is used for [security and system administration], reviewed by [named role], and not used for general performance management.

If this policy is not followed

Deliberate breaches may be treated as a disciplinary matter. Honest mistakes reported promptly will not be. We would far rather hear about a problem within the hour than discover it in a month.

When you leave

All access is removed on your last day and company data is removed from personal devices.

Policy version: _____ **Effective date:** _____

Name: _____ **Signed:** _____ **Date:** _____

Version 1.0, August 2026. Figures in Canadian dollars unless stated. Checked at time of writing; verify anything time-sensitive before relying on it.

Free to use and share. From Brevity.Tech, managed IT and automation for small businesses across Metro Vancouver. brevitytech.ca