

New hire IT setup checklist

Everything that should be ready before a new person's first morning. Work through it in order. Most of it can be done the week before they start.

Free to use and adapt.

A week before

- ☐ Confirm start date, job title, manager, and which team they join
- ☐ Decide what access they need, based on the role rather than on a person
- ☐ Order or allocate hardware: laptop, monitor, dock, headset, phone
- ☐ Check the laptop is under warranty and note the serial number
- ☐ Order any paid software licences they will need

Accounts and identity

- ☐ Create the user account (Microsoft 365, Google Workspace, or your directory)
- ☐ Assign the right licence, not the most expensive one
- ☐ Set the email address and display name to match your naming convention
- ☐ Add to the correct groups and distribution lists
- ☐ Enforce multi-factor authentication before the account is used
- ☐ Add them to the password manager, sharing only the vaults they need
- ☐ Set up their signature and calendar permissions

The device

- ☐ Enrol the device in management before handing it over
- ☐ Turn on disk encryption and record the recovery key somewhere safe
- ☐ Install endpoint protection and confirm it is reporting in
- ☐ Apply all pending operating-system updates
- ☐ Install the apps they actually need, not a default pile of everything
- ☐ Set up file sync or backup so their work is never only on the laptop
- ☐ Record the device against their name in your asset list

Access to systems

- ☐ Shared drives and folders, at the least privilege that lets them work
- ☐ Line-of-business applications, with the correct role
- ☐ Third-party tools: CRM, accounting, project management, VPN
- ☐ Building or door access, if that runs through the same process

Day one

- ☐ Hand over the device and walk them through first sign-in
- ☐ Watch them complete multi-factor enrolment. Do not just send instructions.
- ☐ Show them the password manager and how to use it
- ☐ Tell them exactly who to contact when something breaks
- ☐ Cover the basics: phishing, lost-device reporting, no shared logins

Within the first week

- ☐ Check in and fix whatever was missed. Something always is.
- ☐ Confirm backup or sync is actually running for their device
- ☐ Remove any temporary access granted just to get them started

Two things people get wrong

Copying an existing user to set up access. It feels efficient, and it quietly spreads permissions nobody intended. Copy the role, not the person.

Skipping the asset record. If you do not write down who has which device, you will not know what to collect when they leave, and you cannot prove device encryption to an insurer.

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 run this process for clients so it never depends on someone remembering. brevitytech.ca · 778-321-2372