

Employee offboarding checklist (IT)

What to do the day someone leaves. Speed matters here more than anywhere else in IT.

Free to use and adapt.

Before the last day

- ☐ Confirm the exact departure date and time
- ☐ Decide who inherits their email, files, and responsibilities
- ☐ Agree whether the mailbox is forwarded, converted to shared, or archived
- ☐ Ask what they hold that IT may not know about: subscriptions they signed up for, vendor portals, cloud storage, a company phone account in their name

On the last day, within the hour

- ☐ Disable the account. Disable, do not delete, so data stays recoverable.
- ☐ Revoke active sessions and tokens. Disabling an account does not always sign out a device that is already signed in.
- ☐ Remove multi-factor methods and devices registered to them
- ☐ Remove any app passwords and OAuth app consents on the account
- ☐ Reset the password as well
- ☐ Remove them from the password manager and rotate any shared credentials they knew
- ☐ Remove access to line-of-business apps, CRM, accounting, VPN, and remote access
- ☐ Remove from distribution lists, shared mailboxes, and groups
- ☐ Disable building or door access

The device

- ☐ Collect the laptop, phone, dock, monitors, keys, and access cards
- ☐ Check what came back against your asset list
- ☐ Keep the device intact until you are certain nothing on it is still needed
- ☐ Wipe and re-enrol before it goes to the next person
- ☐ If a device is not returned, lock or remotely wipe it
- ☐ On a **personal** device, remove company data only. Do not factory reset it. That destroys someone's photos and creates a problem you do not want. Selective removal only works if the device was enrolled and the acceptable use policy was signed first

Data and continuity

- ☐ Transfer ownership of files only they controlled
- ☐ Check for automations, scheduled reports, or scripts running under their account
- ☐ Check for anything registered in their name: domains, certificates, vendor logins, software licences, the mobile account
- ☐ Set the mailbox to forward or auto-reply as agreed
- ☐ Confirm a final backup exists

After 30 to 90 days

- ☐ Reclaim the licence once mailbox handling is settled
- ☐ Archive or delete data in line with your retention policy
- ☐ Remove the account permanently, if your policy allows

Access register

Fill this in when someone **joins**, not when they leave. Reconstructing it eighteen months later under time pressure is where things get missed.

System	Access level	Date granted	Date removed	Removed by

The one that costs people money

Anything registered in a departing person's name. The domain, the SSL certificate, the vendor portal, the mobile account. It all works fine until something needs renewing, and then nobody can get in. Check this before the last day, not after.

A close second: shared logins. If the team shared an account, that password now needs changing and everyone needs telling. Which is the argument for not having shared logins in the first place.

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. Same-day offboarding is included in every plan we run. brevitytech.ca · 778-321-2372